DYNAMIC PRIVACY AND SECURITY ASSESSMENT IN A SMART HOME ENVIRONMENT USING BIG DATA ANALYTICS

A THESIS

SUBMITTED TO THE

**TILAK MAHARASHTRA VIDYAPEETH,
PUNE**

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN COMPUTER SCIENCE

**UNDER THE BOARD OF MODERN SCIENCES &
PROFESSIONAL SKILLS**

BY

Mrs. Supriya Vivek Nagarkar
(25315008508)

UNDER THE GUIDANCE OF

Dr. VIKAS PRASAD

DEPARTMENT OF COMPUTER SCIENCE

January 2022

CERTIFICATE

This is to certify that the thesis titled, “DYNAMIC PRIVACY AND SECURITY ASSESSMENT IN A SMART HOME ENVIRONMENT USING BIG DATA ANALYTICS” which is being submitted herewith for the award of degree of philosophy (Ph.D.) in computer science Department of by Tilak Maharashtra Vidyapeeth, Pune is the result of original research work completed by Ms. Supriya Vivek Nagarkar, under my supervision and guidance. To the best of my knowledge and belief the work incorporated in this thesis has not formed the basis for the award of any degree or similar title of this or any other University or examining body upon her.

Place: Pune	Dr. Vikas Prasad
Date:	Research Guide

DECLARATION

I hereby declare that this Ph.D. thesis entitled "DYNAMIC PRIVACY AND SECURITY ASSESSMENT IN A SMART HOME ENVIRONMENT USING BIG DATA ANALYTICS", completed and written by me has not previously formed the basis for the award of any degree or other similar title upon me of this or any other Vidyapeeth or examining body.

Place: Mrs. Supriya Vivek Nagarkar

Date: Research Scholar

ACKNOWEDGEMENT

One of the simplest yet most powerful things humans can do for one another is to express gratitude. Foremost, I would like express my sincere gratitude to many people who have generously contributed to the work presented in this thesis. The thesis has been a long journey, but it wouldn't have been possible without the guidance and support of several people, whom I would like to thank here.

First of all, I would like to express sincere and humble thanks to my respected guide Dr. Vikas Prasad, NICMAR Pune. Words alone are insufficient to express my thanks to him. I owe him a significant debt of gratitude for his invaluable assistance, mentoring, and continual interest in all aspects of my study. It was a joy and a source of respect for me to finish my study under his expert direction. His optimistic personality helped me to become a better researcher and to do study in the manner that is required of a researcher. His kind gestures and gentle approach have boosted my morale on both professional and personal levels.

It was immense pleasure for me to do my PhD work at Tilak Maharashtra Vidyapeeth (TMV). This is a fantastic location with outstanding technical facilities, helpful employees, and a pleasant research environment.

Dr. Deepak Tilak Chancellor of Tilak Maharashtra Vidyapeeth Pune, receives my warmest gratitude for her invaluable leadership, collaboration, and support in all ways.

I'd like to take this opportunity to thank Dr. Geetali Tilak Mone, PRO- Vice Chancellor and Dean, Tilak Maharashtra Vidyapeeth Department of Modern Sciences and Professional Skills, for her cooperation and assistance.

I would like to express my heartfelt gratitude to my close Friends, particularly Dr. Sumita Joshi, Dr. Kalpana Ghatpande for always being there for me as a best friend during my research exploration.

I am Indebted to Dr. Sagar Jambhorkar Asst. Professor, Defence Officer, NDA, Khadakwasala, Pune for motivating me to pursue my PhD.

Words are not enough to express my gratitude to Mr. Rajesh Prasad & Dr. Jayashree Prasad for continuous support, Advice and help throughout my journey.
I would like to show my appreciation to all the colleagues in TMV. I am thankful to Dr. Ajit Ghodke and Dr. Anup Girdhar for his guidance and support.

I thank Dr. Pramod M. kadam, Assistant Professor Assistant Professor, BVU, IMED Pune for his help and valuable support in my work.

I am grateful to Ms. Asmita Namjoshi, Head, Department of Computer Science, Dr. C Sunanda Yadav, Head PhD Department, for their generous cooperation and support in completing this research project.

I expressed my special thanks to Ms. Minal Kalamkar, Dr. Sunita Nikam, Ms. Padma Pande, Ms. Rashmi Dongre for always being with me as a best friend during my research journey

No words are enough to express my gratitude to my parents and in-laws for their blessings and teachings without their firm support to my life and to my spirit, I could not have gone so far.

I owe a debt of gratitude to my husband Mr. Vivek Nagarkar for his unwavering encouragement and support, which served as a major motivator for me. Special Thanks to My Son Sanket for his unconditional Support.

Last but not least, I wish to convey my sincere gratitude to Lord Ganesh for their numerous blessings bestowed upon me and my family throughout my life.

Mrs Supriya Vivek Nagarkar
Research scholar, TMV.

INDEX

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
BD	Big Data
BDA	Big Data Analytics
CAGR	Compound Annual Growth Rate
CCTV	Closed-circuit television
CIA triad	Confidentiality, integrity, and availability.
CO	Carbon monoxide
CVE	Common Vulnerabilities and Exposures
DES	Data Encryption standards
DGPR	General Data Protection Regulation
DIY	Do It yourself
DNS	Domain Name System
DoS attacks	Denial-of-service attacks
ENISA	European Network Information Security Agency
H2H	Humans-to-Humans
H2T	Humans-to-Things
HA	Home Automation
HDFS	Hadoop Distributed File System
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and communication Technology
IDS	Intrusion Detection system
IoT	Internet of things
IPS	Intrusion Prevention system
ISRA	Information security Risk Assessment
IT	Information Technology
LAN	Local area network
LED	Light Emitting Diode
LOC	Loss of control
LOV	Loss of View
M2M	Machine to Machine
ML	Machine Learning
NFC	Near field communication
NoSQL	Not only SQL
OTP	One Time Password
PC	Personal Computer
PIN	Personal Identification Numbers
RFID	Radio Frequency Identification

SDL	Security development Lifecycle
SHAS	Smart home automation system
SHT	Smart home technology
SQL	Structured query language
SRW	Short range wireless
T2T	Things-to-Things
TCP/IP	Transmission Control Protocol/Internet Protocol
TV	Television
UID	Unique Identification number
VPN	Virtual private network
Wi-Fi	Wireless Fidelity
WSN	Wireless sensor Network
SaaS	Software as a service

Abstract

House automation, often termed as "Smart Home Technology" refers to the use of technology to automate one’s home. Through the Internet of Things (IoT), users can manage practically every element of their house with home automation system based on IoT. Smart home technology starts with basic house amenities that have been equipped with communication technology, allowing for some level of automation or remote control. It contains Appliances such as washing machines, refrigerators, and garage door openers, Entertainment systems for the home, System of home security, Air conditioning, heating, and lighting are examples of environmental controls.

The number of smart home devices is predicted to expand at a compound annual growth rate (CAGR) of 16.9% through 2023, when roughly 1.6 billion smart home gadgets will have been supplied. This prediction is consistent with the continued adoption of the Internet of things (IoT) in homes around the world, owing to the prevalence of various smart devices that either replace or supplement standard home appliances as well as the expansion of the feature sets of these devices. However, not everything has to be rainbows and sunshine. Security in smart homes has become extremely crucial as more gadgets enter the market and the information they manage becomes more sensitive. Moreover, not all owners have a thorough understanding of the IoT devices they connect to their home networks, yet alone security risks that may occur as a result of their use. This could justify the emergence of a new species of cyber threats with different, often unexpected implications.

The security and privacy problems of the Internet of Things (IoT) come from the unique properties of IoT networks. These features include an unmanaged environment, heterogeneity, the requirement for scalability, and resource constraints. Recent cyber-attacks have proved that smart houses can contribute to attacks that can have serious effects for both its users and society. Although there is a lot of effort being done to discover security solutions for IoT and smart homes, there is still no clarity on which solutions are best. To solve these issues, a deeper knowledge of the house and its security measures is essential.

The results of a survey Thesis conducted with the purpose of better understanding the security and privacy concerns of the Smart home Environment are presented. The main focuses on gaining a better knowledge of home security practises and how they might guide the design of appropriate security equipment to support them.

This research aims to address the topic of smart home user security and privacy by questioning a sample of Home users about their concerns and thoughts on the subject.

The study demonstrate how existing IoT security solutions are insufficient, and that there are several faults and risks to end users. The study will look at the issues and provide an analysis for future research efforts so that a better informed conclusion may be made.

For the purposes of this study, no data analytics tools or associated technologies will be used. The focus of this thesis is on the privacy and security of smart home settings that use big data analytics. Analytics over massive data (produced by the Smart home ecosystem) is required for a long-term smart house. The smart home service providers/vendors are responsible of this part of the service.

The work was conducted in three steps:

(a) Through a survey of 396 participants, an empirical investigation of security support behaviour and variables that impact the result of security decisions in the home was conducted.

(b) Construction of a framework Safe@Smarthome to assist the design of home security technologies

(c) Validating the defined framework is validated using case based approach

CHAPTER 1
INTRODUCTION

CHAPTER 1

INTROUDCITON

1. Introduction

"Anything that multiplies conveniences multiplies threats as well," says Prime Minister Narendra Modi.

1.1. Overview

Modern civilizations expect their lives to be improved by new ideas and new technologies. Internet has brought dramatic changes in people's lives. Evolution Internet of Things (IoT) has huge potential to improve overall quality of life. Under present condition, IoT has entered in every field ranging from agriculture, manufacturing, healthcare, smart cities and our homes too. With IoT, modern homes have become more technology enabled, which could potentially generate comfort, convenience, protection, safety and security. Despite the strong and accepted concept of "Smart Home" in other countries, there are obvious hesitations in India. For home owners their personal belongings and physical asset both are most essential. They are afraid of losing their personal assets, information/ data which may be stolen and put to wrong use. Therefore, protection of confidential information and physical asset is their top priority.

India is a country where technology is in transition to make its impact. However very few people really understand the power of it, while most other just use it without knowing the pros and cons. This lack of knowledge / partial knowledge most of the times gives rise to an imaginary problem. Under the circumstances, concerns about security and privacy seem to be legitimate. The usage of methodologies like data analytics helps in presenting a true picture which in turn can help to define the counter measures to help the concept of smart Homes to succeed.

In the country like India, where the technology is still progressing, concept of smart home will take time to make its influence. Yet very few people really understand its power, while most people just use it without understanding its pros and cons. This lack of user's knowledge often results into hypothetical problems. Hence the security and privacy issues are real. Application of methodologies such as data analysis can aid its selections.

1.2. A Generic view of Smart Home and concept

Home automation and the Internet of Things (IoT) are getting popular day by day. In present days automated systems are most liked over the manual system. Smart Home is an IoT domain. It is a concept of creating a pervasive environment that comprises network of devices including wireless sensors, connected devices and related technology to provide in house network access.

This setup provides home residents an ability to obtain knowledge, monitor and automate various parts of home. This enhances the efficiency of day-to-day household activities; maybe from anyplace, anything, anywhere and anytime, using internet via a smart phone application. With advancement in smart home technology, smart devices become networked to form digital mesh of intelligent home ecosystems. These ecosystems have connected devices to combine efforts and offer benefits beyond convenience including enhancing the security and safety, culture, health and fitness of the residents and their overall quality and efficiency of the lives. The advancement of IoT and smart connections in present days home, has gained popularity owing to maturity in the use of data analytics, wireless sensor protocols, wireless sensors, advanced processor, edge computing, and widespread availability of mobile network.

Smart home is a major component in Smart City. As every other IoT, the aim of IoT enabled home is to make the life of home owner simpler and more comfortable.

Home IoT devices can be categorised into following Types

1. Communication devices - Personal Computer, Tablets, Smart phones
2. Entertainment devices – Smart TVs, Projectors, Sound bars , Speakers streaming devices
3. Home gadgets – Smart Oven, Refrigerator, Dishwasher, Robotic vacuum cleaner etc.
4. Smart lighting – Bulbs , Plugs
5. Security devices – Smart locks, Surveillance CCTV camera, Video Door phones,
6. Wearable's – Fitness trackers,

Most of the IoT devices commonly used by smart home users are included in the above list. However, since this market is very dynamic new products are being developed and launched almost on a daily basis. Therefore, this list is expected to expand exponentially. Given the ease and convenience of these devices, home IoT devices pose a major danger to home owners. Risks of inadequate protection may have a very significant effect on home owners.

1.3. Smart home market statistics (Global to Local)

Smart home statistics reveals that a rising number of individuals are enjoying the benefits of home automation systems, such as confront and remote access to all of their appliances and many more. After all, cutting-edge technology is handling the majority of the work in their home and a security system that provides the best possible safety for their family. (Source https://comfyliving.net/smart-home-statistics)

Key smart home Statistics

- Globally, there are an approximately 175 million smart homes.
- Generic global trend

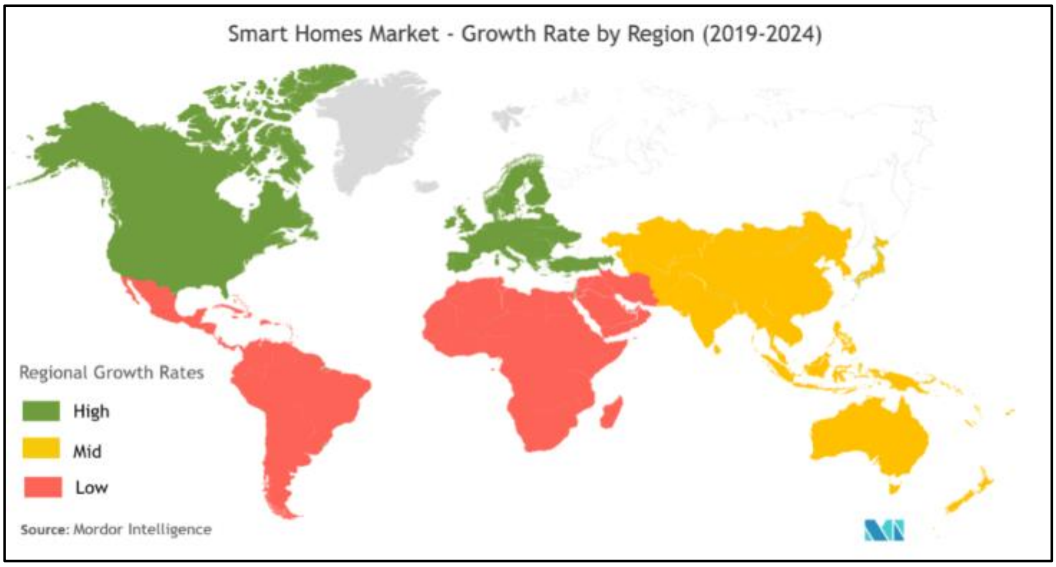

Smart Homes Market - Growth Rate by Region (2019-2024)
Regional Growth Rates
🟩 High
🟨 Mid
🟥 Low
Source: Mordor Intelligence

Figure 1.1 Global Smart home Market Industry

Source: https://www.mordorintelligence.com/industry-reports/global-smart-homes-market-industry

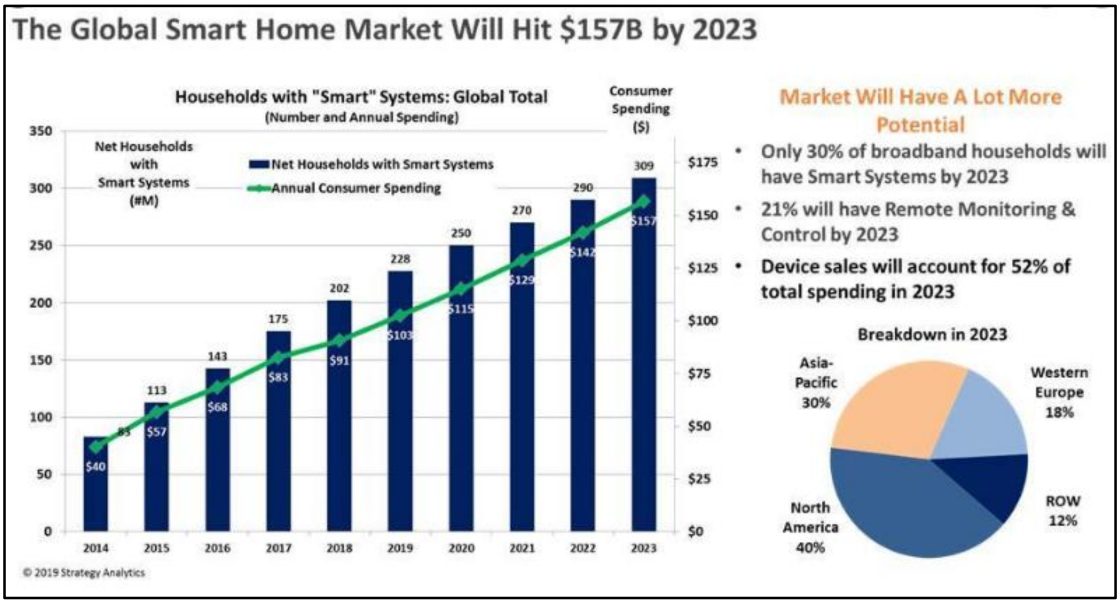


Figure 1.2 Net Households with smart system and annual customer spending

Source:https://www.businesswire.com/news/home/20190925005582/en/Strategy-Analytics-Global-Smart-Home-Market-to-Surpass-100-Billion-in-2019

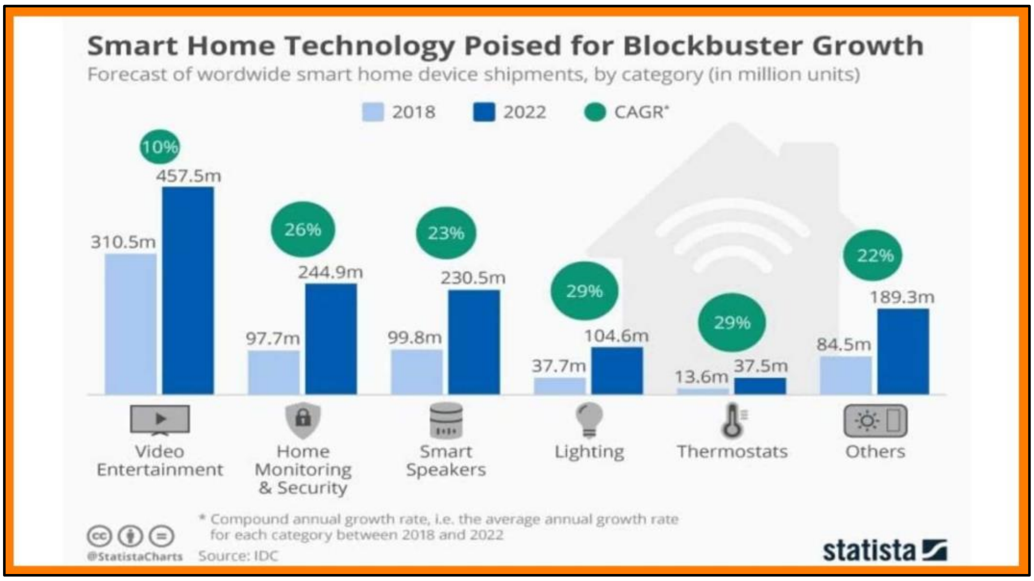


Figure 1.3 forecast of worldwide Smart Home devices

- **Details for American continent**

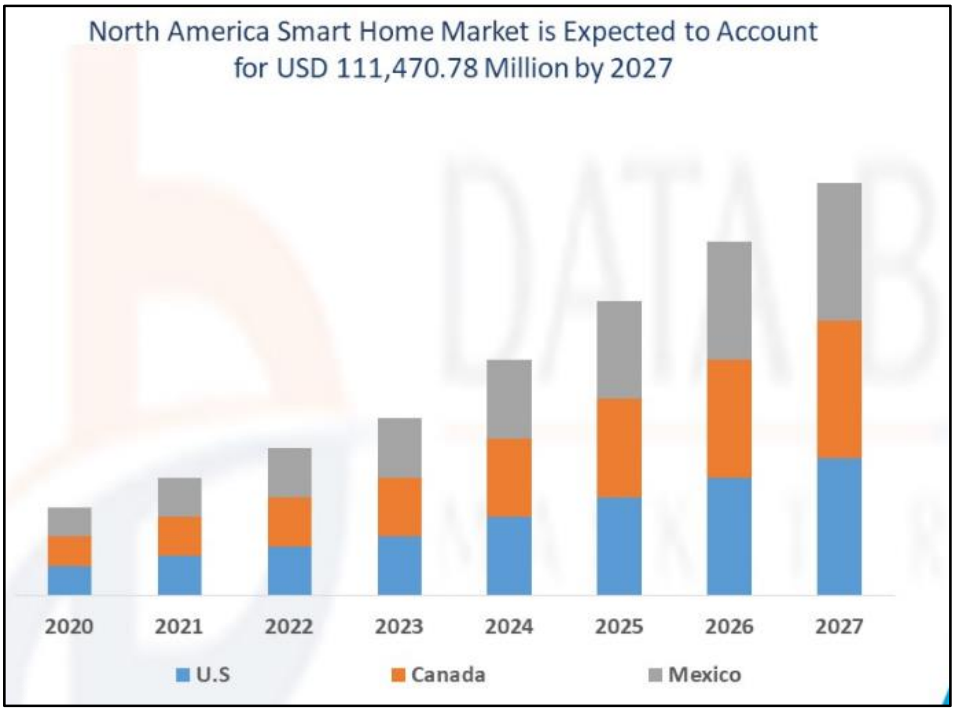
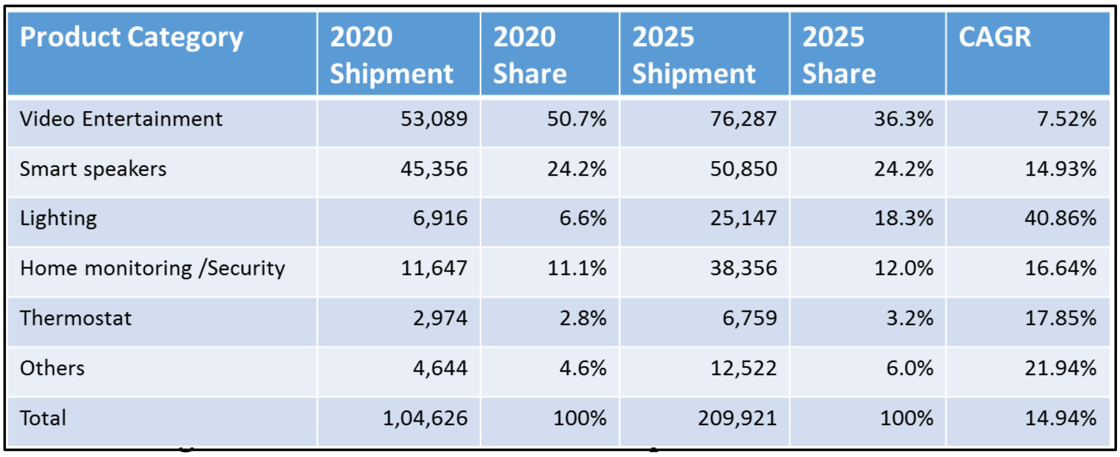


Figure 1.4 Smart home market America

Source: https://www.databridgemarketresearch.com/reports/north-america-smart-home-market

Details for Europe

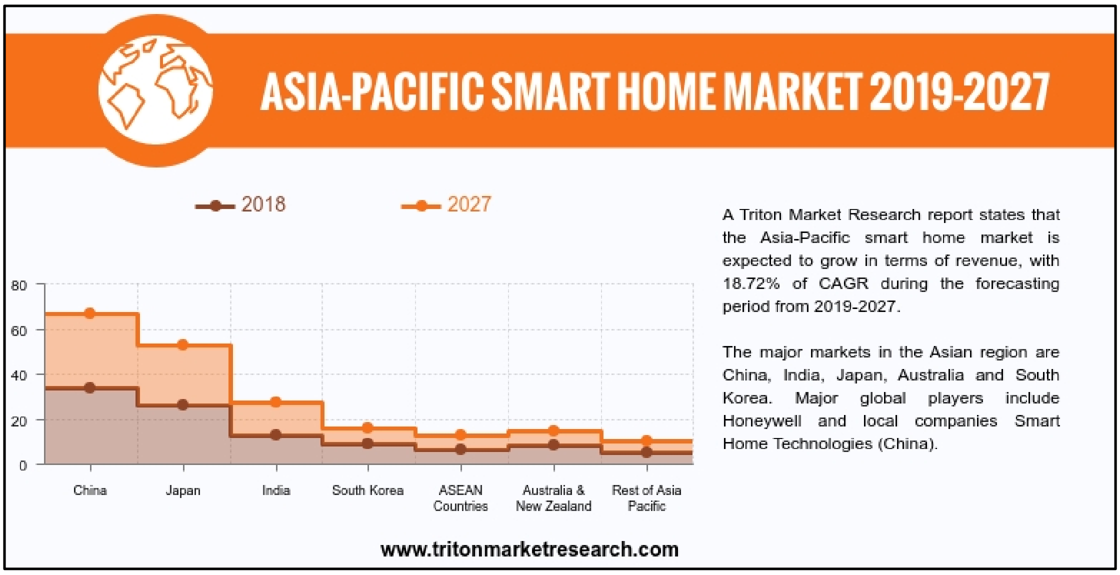
Europe Smart home Devices Forecast by category 2020-2025 (Shipment in Thousands)



Product Category	2020 Shipment	2020 Share	2025 Shipment	2025 Share	CAGR
Video Entertainment	53,089	50.7%	76,287	36.3%	7.52%
Smart speakers	45,356	24.2%	50,850	24.2%	14.93%
Lighting	6,916	6.6%	25,147	18.3%	40.86%
Home monitoring /Security	11,647	11.1%	38,356	12.0%	16.64%
Thermostat	2,974	2.8%	6,759	3.2%	17.85%
Others	4,644	4.6%	12,522	6.0%	21.94%
Total	1,04,626	100%	209,921	100%	14.94%

Source: https://www.neowin.net/news/idc-smart-home-market-to-reach-210-million-units-in-europe-by-2025/

Detail for Asia



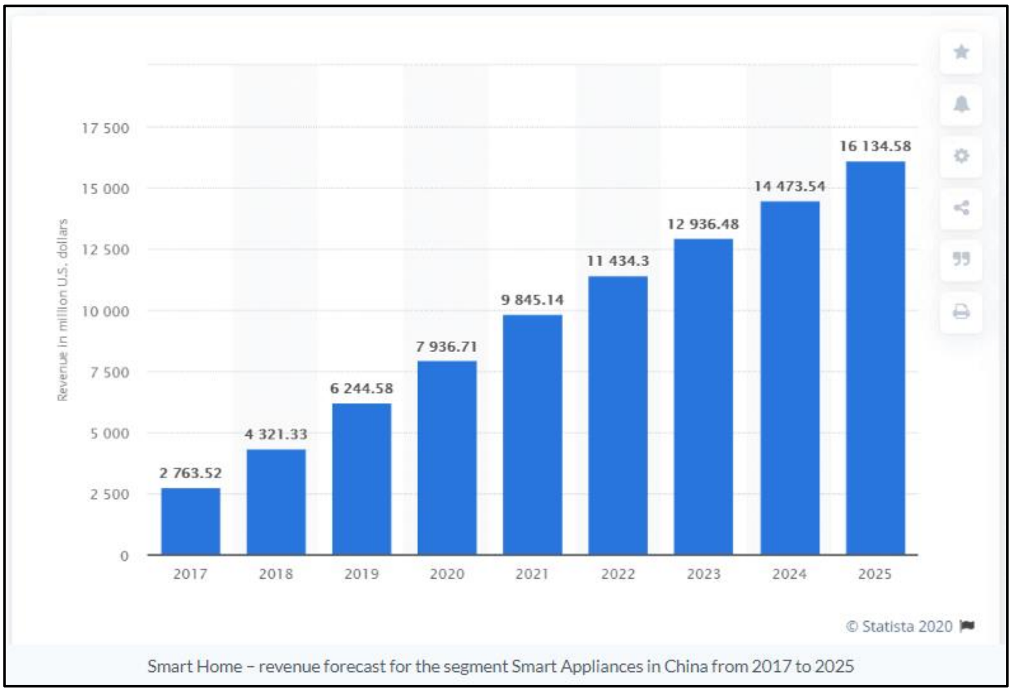
A Triton Market Research report states that the Asia-Pacific smart home market is expected to grow in terms of revenue, with 18.72% of CAGR during the forecasting period from 2019-2027.

The major markets in the Asian region are China, India, Japan, Australia and South Korea. Major global players include Honeywell and local companies Smart Home Technologies (China).

Figure 1.6 Smart home Market Asia-pacific

Source:https://www.tritonmarketresearch.com/reports/asia-pacific-smart-home-market

Details for China



Smart Home – revenue forecast for the segment Smart Appliances in China from 2017 to 2025

Figure 1.7 Smart appliances market China

Source: https://marketingtochina.com/china-smart-appliances-market-is-blowing/

Details for India

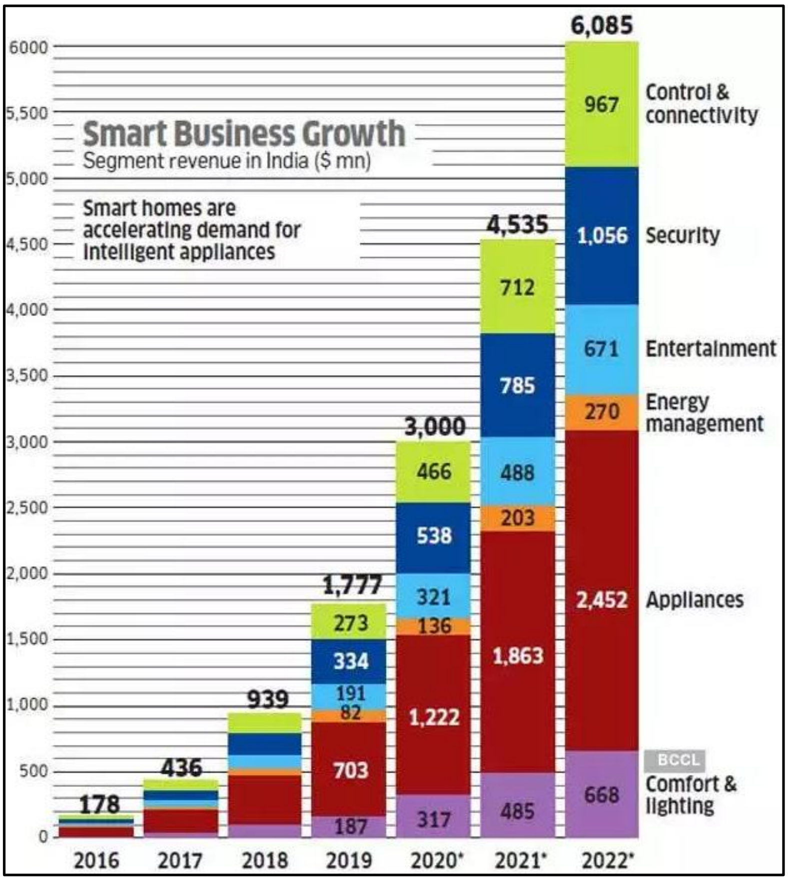


Figure 1.8 Smart home Market India

Source: https://economictimes.indiatimes.com/tech/software/home-smart-hometheindiasboominghomeautomatiomarket/articleshow/74630996.cms?from=mdr

- By 2022, the United States is predicted to have 63 million connected homes.
- From 2020 to 2025, the global connected home market is expected to develop at a CAGR of 25%.
- Amazon has the largest market share in smart devices, and it will continue to do so until 2021.
- Smart heating and cooling systems can help smart home owners save significant amount of their energy bills.
- Majority percent of home owners desire smart security systems in their smart homes.

- According to smart home statistics in the United States, approximately 35% of US internet households experienced a data security issue in the year 2020.
- At least one device in 40.8 percent of smart homes is vulnerable to cyber-attacks, putting the entire home at risk.

Statistics about the Smart Home Automation Industry in the World

- As per Statista, Investopedia**,** Globally, there are an estimated 175 million smart homes.
- As per Statista, The United States has the smart homes after that china is in the second position. Germany, the United Kingdom, and France are driving the market forward. Japan is also struggling to take hold on smart market.
- So far this year, the worldwide smart home market has earned $90.97 billion in sales.
- From 2020 to 2025, the global connected home market is expected to develop at a CAGR of 25%.
- According to home automation system statistics, smart entertainment systems are found in 44% of smart homes.
- 63 percent of respondents polled desire smart security systems in their smart homes. As per time survey, Home monitoring and security solutions will account for 22.6 percent of the smart-home industry by 2023.
- Energy monitoring market value is expected to increase at a CAGR of 26% from 2019 to 2026.

Indian smart home market statistics

India has been one of the fastest expanding digital market due to lower data costs, increased disposable income, and lower hardware prices. Technology has taken spot light in all aspects of life, including home design, in the effort to making life easier and safer. (Source Statista Research Department, Apr 7, 2021)

- As per allied market research Indian market size forecasted to reach $13574 million by 2026 at CAGR 29.8%

- Lighting, security, audio/video, and HVAC are the four functional categories of home automation in India today. The greatest component of the residential market is lighting, while the main component of the commercial market is security.
- Cities & Market share in India

Cities	Market share in %
Pune	15%
Delhi	13%
Mumbai	12%
Hyderabad	9%
Ahmedabad	7%
Bangalore	7%
Chennai	6%
Jaipur	4%
Kolkata	4%
Ludhiana	2%
Chandigarh	2%
Cochin	2%
Coimbatore	2%
Other	15%

Table 1.1 Cities & market share in India

Major Features of Indian smart home market

Technical report on M2M/IoT enablement in smart homes has explained the Indian Market landscape. Points listed below are some of the key features of the Indian smart home market.

- **Huge Opportunities in the Emerging Indian Market**

  Subscribers are predicted to surpass 400 million in the current year, thanks to the rise of the Smartphone market and its availability at low prices. Internet penetration will aid in the creation of an eco-system for many M2M/IoT verticals, including Smart Homes.
- **Start-up opportunities**

Many start-ups and people are developing and using home automation platforms in the Do-it-yourself (DIY) category. Several sensors are now common fitments for development platforms, which is assisting many developers. The limitation is that the Indian market, or Smart Homes, does not have a standard or even a preference for a particular standard or technology as yet.

- **Low market Adoption**

  In India, the Smart Home market is currently restricted. Currently, the market caters mostly to the higher income group. Home monitoring and security products are being purchased by an increasing number of people. Home automation features are already included in the apartment leases in newer buildings. However, there is a widespread misunderstanding regarding home automation technologies and how they might be used**.**

- **The IoT market-Data Driven Market will be led by big data analytics and cloud services**.

  When a large number of devices work at the same time, a large volume of data is generated. In the Indian Smart Home market, processing this organised and unstructured data is a challenge, but big data framework may be seen as an opportunity.

- **Positive support from Government**

  In a program leading, the Indian government intends to build 500 smart cities. In the first phase, 100 cities will be constructed, with 20 of these cities being identified in the initial list. A second and third list of 13 and 27 cities, respectively, was recently announced. As smart homes are an important component of a smart city, the market is favourable for smart home service providers

- **With an increasing number of gadgets, cyber security is gaining adhesion**.

  As the Internet of Things (IoT) spreads, more and more connected devices will arrive in the market. The greater the numbers of devices, the more secure the security features would be to safeguard against attacks. This presents a business opportunity for cyber security firms.

- **DIY kits are increasing popularity, and e-commerce is helping to boost sales.**

In India, Do It Yourself (DIY) kits are gaining popularity, and many Smart Home aficionados have already purchased and installed these gadgets. Smart sensors that can be connected into home appliances and controlled remotely using smart gadgets are included in these packages. These kits are now readily available at reasonable prices on e-commerce websites**.**

- **Smart Cities Exhibitions helps to popularise Smart Homes**

  Exhibitions, workshops and assemblies on smart homes are being held across the country to promote the concept. The statistics from these events show an increase in the number of visitors to the stalls as well as the number of merchants /exhibitors.

1.4. IoT based Smart homes - Fast growing list of Applications

Technology has been rising at an insane pace, and isn't even going slow. Things from science fictions are becoming reality now – thanks to technology. Smart home technology has only been around for a couple of years. Bill Gates began constructing his smart home in 1988 and ended up in 2005. Now neither you have to be rich enough like bill gates nor will it take 17 years to build your smart home. Now many options are available like Central control unit, Smart home application based home.

The following are the most commonly used Gadgets for Smart Home.

Leisure & comfort – Ability to remotely control the equipment to improve the comfort is an important aspect. Equipment's like lighting, music, air conditioning system play important role in the in improving the comfort.

1. **Smart Lighting controller -** Smart lighting is an energy-efficient lighting technology. This can involve high performance and automatic controls that allow changes on the basis of energy efficiency. This can involve high performance and automatic controls that allow changes on the basis of factors such as occupancy or availability of daylight. Lighting is the intentional application of light to achieve some desirable or functional result.
2. **Smart wireless speakers** - The Indian wireless speaker market is projected to hit a CAGR of 10% over the 2020-2025 forecast periods. Smart speakers can do so much more than just play music, even though they're doing an outstanding job. They can connect through the internet, tells you about weather, send you the news updates, work as a personal assistant, and serve as a central control centre for your entire smart home system. Alexa, Siri voice assistant, Google assistant, and Bixby are some of the popular products. With the right voice assistants, one can monitor almost every component of home with voice command.
3. **Smart thermostats (air-conditioner) -** Smart air conditioners allow users to remotely regulate the temperature of their home via smart phones or internet-connected devices. It offers energy-saving features along with comfort. These systems also learn the actions of homeowners and automatically change the settings to provide residents with optimum

comfort and productivity. The technology used is wireless sensor network along with and machine learning.

4. **Smart TVs -** Smart TV has become even more dynamic now. The internet TV and the processing unit are providing more information to discover. Smart TVs can be wirelessly connected to several input devices to improve usability and power. Wireless keyboards and mouse, smartphones and tablet PCs can all be paired to enable text entry, navigation and web browsing. Smart system comes along with built-in features like camera and microphone which enables face and voice recognition. There are TV-related threat that gathers and stores a lot of private data that is again connected to the privacy and protection of users.
5. **Smart video door bells** – Door bells not only notice and warn when someone is at the front door, but they can also send you video clips of who's there, and they can use intercom technology to speak to your guest. Home owner can see it from mobile screen, or even ask smart speaker to display the image.
6. **Robotic vacuum cleaner** - The robotic vacuum cleaner instantly cleans floors without human intervention. This beautiful gadget travels around the table legs and corners of where it's vacuuming. One can even clean the home whenever the person is away from home.

Home security - The main aim of home security system is to provide simple solution to home and second homes protection altogether with a device that would be handy and user-friendly, including both a 24/7 surveillance and an alarm security system. There are various types of items, including the good old CCTV system, the standard alarm system. Getting a protection system greatly reduces the chances of burglary on your house.

1. **Surveillance camera** - Security cameras are designed to keep home and home owner’s safe. Surveillance camera is a stand-alone, self-contained visualisation device that allows users to capture high density video and adapt to changing light levels during the day. It also provides camera software, such as Wide Dynamic Range, which balances the light in the video after it has been captured, or video

compression to allow users to store more data. The technology used is the processing of images.

2. **Alarm System** - If the worst happens and your home or company is destroyed, the alarm can be set to go off. Many devices can also be set up to notify the authorities automatically.
3. **Automated Locks** - Most of the burglars come in through the unlocked door or window. Using automatic locks to lock your doors from your smart device remotely.
4. **Fire/gas/Flooding sensors** – House Theft wasn't the only danger to your home or company. Fire, gas, and water may also cause severe harm. Smart fire / CO detectors provide in-app silencing and, if activated, send alerts to your computer. They're a little easier to look at, too, than your typical detector.

Smart kitchen - Smart kitchens, they typically apply to something connected through IoT (Internet of Things) technology, Bluetooth, or Wi-Fi. Since smart devices are linked, they can be remotely operated via a mobile app or a voice assistant like Amazon Alexa or Google Home Assistant. When it comes to cooking, smart products can make things more effective, more accurate and safer.

1. **Smart Refrigerators -** Smart refrigerators feature internal cameras, more customizable user-controlled cooling options, and the ability to connect with your smartphone or tablet when away from home. It will allow the inventory of all perishable food to be preserved. Along with these details, the energy-consumption details of the refrigerator are visible. It has a variety of applications, such as the food manager and the supermarket application, which allow you to make your shopping list accessible on a stock basis. The technology we use is wireless communication and Artificial Intelligence (AI).
2. **Smart Dishwashers** - Smart dishwashers run on software similar to smart ovens compatible with the app. With these apps, you can check your wash status, get updates when loading is completed, and stop /

start loading. Similar to the oven and refrigerator, most of these apps can also run diagnostics on your units, if required.

3. **Smart ovens** - Smart ovens allow you to monitor your operation from anywhere. There are also smart ovens that can be powered by Alexa. Some apps also allow you to look up recipes and queue up the time and temperature required for them, but sometimes you will need to click the start button.
4. **Smart Cookers** - Power your smart rice cooker from your phone or tablet. You can check the temperature, adjust the settings, and turn it on and off. It makes the easiest cooking appliance even more convenient.
5. **Smart Coffee machine -** Most coffee pots can be set to a timer to start brewing when you want to. You can tell smart pots to brew from your phone so that you can start a pot whenever you want coffee.

   In addition to this there are many Devices like Smart washing machine and dish washer that start/stop/pause a load, check on the status, and receive a notification when the load is finished. Also Smart plates and forks that control calorie intake, and link to the app to help keep track of what person is eating.

Smart medication care - Home Automation can provide inexpensive alternatives that allow peace of mind and independence for your loved one. Monitor as little or as much as you like you need to. Some of the most common choices for home automation medical treatment are –

1. **Video Surveillance -** Video Monitoring helps you to check in from the comfort of your smart device on your beloved one. You will achieve sense of security with video surveillance, ensuring that your loved one is safe at home.
2. **Alzheimer's patient care** - The majority of Alzheimer's and Dementia patients' are away from home or living facilities. It's a terrific experience for them and for you when this happens. Home monitoring systems will help ensure that this doesn't happen by notifying you on your mobile when someone is leaving or entering the building.

3. **Medical alert system -** Health Alarm buttons are lightweight, waterproof buttons that your loved one can wear around his neck, on his wrist, or even just bring with them. The button connects to an intercom system that, when turned on, calls a medical monitoring centre. If required, anyone in the call centre will warn you or the patient's emergency services. Some buttons may also feel when the user has dropped and warns the call centre automatically.

Pet care - Caring for your fur-babies is simpler than ever with smart pet-tech. The best part of these devices is that they make life simpler for you and your pets. Feel less guilty about keeping them home alone for most of the day, and enjoy that much more time you spend with them.

1. **Video monitoring -** Use of video cameras with related app allows you to check your pets while you're not at home. Special pet-oriented monitors do more than just let your pets watch. Many of them can see and hear you as well. Unlike other cameras they send you general motion and sound warnings, just lets you know about important pet-related events.
2. **Smart Pet Doors - Smart** Pet Doors operate with a smart key on your pet's collar. They just let the animals with the key in and out of the house, so that no unwanted pets can enter in the home. You can even lock the door when you don't want your pet to go out.
3. **Self-cleaning litter boxes -** Pet care is made so much easier by self-cleaning litter boxes that wash, sanitise, dry and fill themselves. They also have litre boxes disguised as cabinets, in order to be completely out of sight.
4. **Smart Feeders** - Smart feeders automatically provide food and water to pets. It is easy to schedule feeds and monitor portion sizes for fur babies using the phone based software apps.

Smart Bathrooms - The most basic needs can be improved in the Smart Home. Smart bathroom technology will enable your bathroom more than the space you need to use.

1. **Smart Bathrooms** – Smart Toilets: Smart toilets provide basic features such as touch-free flushing, tray-opening sensor, automatic bowl cleaning and sanitising. They also have some lavish features, such as a built-in bidet, heated seats and more.
2. **Touch free soap dispenser –** Allows you to take extra care when it comes to preventing germs is with this great touch-free liquid soap pump sensor from Simple Person.
3. **Smart shower with speaker** - Smart Showers do have range of capabilities. They can be switched on from the comfort of your bed before you even wake up, except your ideal shower setting, and some even have a TV in them.
4. **Human sensor mirror - These** mirrors light up when you approach it. These system

1.5. Smart homes: Security & Privacy

The European Network Information Security Agency (ENISA) (2015) identified emerging risks associated to all product and services and suggested good practises to mitigate them.

1. **Cyber-attacks** - Usually, a physical attacks threatens all assets (devices, Gateways, sensors and also information asset). This form of attacks tamper with hardware parts. Due to the unattended and dispersed nature of the IoT, most systems usually work in outdoor conditions that are highly vulnerable to physical attacks.
2. **Access attacks** - Unauthorized individuals shall have access to networks or computers to which they have no right of access. There are two main forms of access attack: the first is physical access, which enables the attacker to access a physical computer. The second is remote access, which is performed on IP-connected computers.
3. **Tracking**: User movements can be detected by the device's unique identification number (UID). Tracking the location of users allows the detection of users in cases where they wish to remain unknown.(Cyber security & IoT Vulnerabilities, Threats, Intruders and Attacks 2015)
4. **Physical attacks** - Emerge from a well-identified threat actors like physical disruption of machines. They can lead to different types of risks, including those listed below as Immoral Activity / Abuse or Eavesdropping / Seizure / Hijacking. Typically, a physical assault threatens all possessions.
5. **Reconnaissance attacks** – In general Reconnaissance attacks are information gathering attacks. Unauthorized exploration and mapping of systems, resources and vulnerabilities. Scanning network ports, packet sniffers, Network traffic scrutiny, and sending queries about IP address information are some of the examples of attacks reconnaissance.
6. **Accidental damage -** It may result from incorrect mutual relationships, or it may result in insufficiently skilled people. As this could have an effect on the controlling capability, the possible effects also include the data leakage, unauthorised alteration or loss.

7. **Eavesdropping/Interception/Hijacking** - these are related to both privacy and cyber security threats. By exploiting design or implementation vulnerabilities, the intruder will compromise one or more properties, whether the loss of confidentiality of private data or the loss of control of the system. Most security good practises are aimed at counteracting these situations.
8. **Denial-of-service (DoS attacks)** - This form of attack is an attempt to make a computer or network resource inaccessible to its potential users. Due to low memory capabilities and restricted processing power, most IoT devices are vulnerable subject to resource weakness attacks.
9. **Access attacks** – Unauthorized individuals shall have access to networks or computers to which they have no right of access. There are two main forms of access attack: the first is physical access, which enables the attacker to access a physical computer. The second is remote access, which is performed on IP-connected computers.
10. **Identity theft** - Identity theft happens when somebody, without their permission, uses another person's personal identifying information, such as their name, social security number, or credit card number, to commit fraud or other crimes. Through exchanging limited personal details with smart devices and constantly reviewing your credit report for negative changes, you will reduce the risk of a data breach impacting you.
11. **Intrusion into Home (house braking)** - Security flaws in any of these devices might allow hackers to disable surveillance or unlock doors in order to let in suspects, burglarize your house, or even lock you out of your own home. Installing security door props and a smart security alarm will help prevent intrusions.
12. **Personal recordings** - According to cyber-security experts, a bug in Amazon's Alexa smart home devices may have given hackers access to personal information and conversation history. Without the owner's knowledge, attackers may install or uninstall apps from a smartphone.
13. **Loss of confidentiality** - Threats to confidentiality are those that result in the unintentional leak of sensitive data. Confidentiality breaches in home monitoring systems, for example, can result in the unintentional disclosure

of sensitive medical data. Unauthorized system access is a hazard if confidentiality is lost in things like keys and passwords.

1.5.1. What is privacy?

The right to privacy is a fundamental human right. Privacy refers to the right to control your personal data. The right to privacy is the ability to be left alone. The right to freely move and associate. Individual autonomy is provided through privacy. One of the key advantages of privacy is self-sufficiency, or freedom from external influence and control. Respecting a person's privacy implies respecting their autonomy. Developing an individual identity necessitates privacy. Privacy can also be defined as a state of being shielded from unauthorised access by others, whether it is physical access, personal information, or attention. With Smart home, privacy is a major concern. Smart home identified specific usage data, which could result in the disclosure of information about specific devices used in homes. This can lead to the development of profiles of the user's behaviour. The capability to get device usage data is the users’ privacy concern. The valuable consumer data that may be utilised to learn more about the user's lifestyle. There are some types of data that can be treated as privacy threat.

- Important contact details
- Financial details of the users
- Data generated from smart gadgets
- Health related information

Need for Users privacy in smart home context

The threats to user privacy are an important topic to investigate in smart homes. As more sections (and gadgets) of the home become connected to the internet, users and other stakeholders can have access to the entire system i.e., the home, rather than simply individual gadgets. This means that not only physical devices might be linked, but that these devices, as well as the numerous stakeholders involved, may get access to live smart home data. Finding effective techniques to give consumers with a full image of the entire system, as well as an indicator of the sensitivity of data in transit, while also assisting the administration of telecommunications networks, is a big challenge. Digital footprints left by users (more or less freely) when using a smart home system can give meta-information about family members' activities, allowing for the creation of substantial individual and collective profiles of a house's residents. Aside from the potential for physical harm, there is also the possibility of psychological harm. The concept of the home as a private domain, for example, may no longer be accurate in terms of burglaries. Instead, the house might become a public space where the firms behind linked devices learn more about a resident than his or her closest friends or family. In addition to the potential physical consequences, such as increased burglaries, the notion of the home as a private space may no longer be accurate. Instead, the house may become a public space where the firms behind connected gadgets learn more about a resident than his or her closest friends or family. It would be interesting to investigate the sensitivity, as well as the potential risks factors, associated with how personal information is managed in the home setting and the ecosystem of humans, technology, information, and actors involved. The inclusion of social behaviour of human players as a friendly users and as criminals is a critical feature in this research. Another exciting area to investigate is user-generated information management strategies in smart homes. The Methods for minimising information sensitivity, such as customizable privacy as well as data minimization and management, should be included in an analysis. The crucial challenge is where to draw the line between public and personal information, as illustrated in the scenario of how to manage a surveillance camera. Instead of a fixed border, it would be preferable if users could easily and transparently configure the system to their own privacy preferences.

A viable option is to use good practises to guide end-users through this process. Another important issue related to the scenario of system functions and data connection is how information is collected, saved, and handled, as well as what laws, policies, and standards govern this. Considering the glaring feature of accidental or intentional privacy breaches, as our scenario of misuse of user-intense gadgets shows, it is of course critical to maintain legal compliance. Technical methods governing access to collected data and how such access might be sought are also a major source of worry. Transparency in data sharing and usage contracts, such as user data management services, proper service level agreements with third-party actors, and techniques for promoting awareness of the possibilities, as well as the risks, associated with smart home automation systems are all required.

1.5.2. What is security?

As defined by Laura Shepherd and Jetta Weldes, (2008), the security is "The state of being free from danger or threat. It is freedom from the possibility of harm, danger, or loss. All of the procedures taken to secure a place, or to guarantee that only persons with authority enter or leave it, are referred to as security. Security is also associated with Safety and liberty. Confidentiality, integrity, and availability are the three basic security objectives for data and tangible ICT resources. Confidentiality is a piece of private and exclusive information can only be viewed by authorised individuals. Integrity is only authorised individuals can create, alter, or delete data. The term "availability" refers to the ability to access data or the system itself when the authorised user requests it.

Security threats

- Eavesdroppers who are interested in their neighbours' actions.
- Eavesdroppers with a vested interest in gathering information for nefarious intentions.
- Proactive attackers looking to launch large-scale attacks. Terrorists are included under this category.
- Intrusive data management companies who wish to utilise your personal data to create user profiles and sell them to marketers.

Need for security in Smart home Context

Security should always be a top priority, and it should be emphasised at all times. A common interface of a smart home automation system is the subject of a research effort involving prominent industrial actors in the segment of Smart Home Automation System (SHAS). It is feasible to transparently control many smart home automation systems in real-time using SHAS. Third-party stakeholders, such as property owners and municipalities, can also monitor and regulate energy use and technological gadgets in houses and buildings remotely.

The application of Information Security Risk Assessment (ISRA) tries to help to bridge the gap between risk analyses and the design and development phases of smart home automation services and technology. In terms of virus mitigation, access control, and leakage of confidential information, security in design is critical for preventing and regulating dangers posed by IoT-connected homes. As a result of the smart home systems' ability to link to other home devices, each with its own function, the original view of security requirements (if any) may be discarded. Furthermore, security considerations for IoT product development for the connected home must encompass indirect features such as connectedness, Interoperability, and ubiquity. Smart home system is often part of a larger ecosystem of vendors, users, systems, and so on, and the number of potential cyber-attack surfaces grows at the same time as they becomes more physical. Data management is another crucial part of the smart home that should ideally be addressed throughout the planning process. A lot of data is in transit with smart home systems. Though this data is often generated by or for the user, it must be considered that a major portion of it is personal and sensitive. Because of the dynamic nature of smart homes, in which the configuration of system-connected devices changes over time in unpredictable ways, it is critical that this feature be considered early in the system development process.

Despite the difficulty of include all of the above listed components in the design phase, the goal of involving security specialists and system developers in the application of ISRA on SHAS was to highlight the importance of security in system development. This suggests that there were no theoretical barriers to along with such factors into the design and development.

1.6. Indian Smart home Market

Recently the smart home market in India has significantly expanded from 2014 according to "India Smart Home Market Overview, 2017-2021. The concept of digital homes has gained popularity among urban occupants. Automation in homes is now a reality, and it is much more economically rational, due to technology advancements and cost-effectiveness.

Mr. K Malik, Country Head – MediaTek India, believes that with rapid urbanisation and the government's push for smart cities, the future looks bright. It is clear that infrastructure would need significant technological improvements. We've already noticed that this change is coinciding with an increase in demand for smart-home technology among urban residents. Convenience, entertainment, mobility, and security are all goals of smart home technology, which aims to provide customers with always-connected solutions.

According to Statista, the Indian smart home market is projected to reach $6 billion by 2022, a two-fold rise from the $3 billion forecast in 2020. By 2022, the figure is projected to rise to $53.45 billion globally. Smart homes are dwellings that are designed and built with information and computing technology that anticipates and responds to the owner's needs in a timely and effective manner. People are quietly shifting to smart equipment in Indian households as they search for more gear that can handle regular tasks like running lights, fans, air conditioners, heaters, air conditioner, Smart door locks, and Video cameras etc.

With home automation technology, users can track and manage the functions of smart home devices. Smart home technology can be classified as wireless and wired technology. The wireless technology consist of Bluetooth and WI-FI. Whereas wired system incorporates sensors, internet cablese etc. The main advantages that brings through home automation is convenience, economical, cost effective, safety & security. Protection and energy efficiency are the two most important factors to consider when implementing home automation in India. Home automation system allows user to monitor your home's heating and cooling systems, Furthermore, lights can be turned on and off automatically during daylight and sundown, also when leaving and entering a room, which saves you a lot of money on electricity. One of the deciding factors in the Indian smart home market is cost effectiveness. Metropolitan cities in India Delhi, Mumbai, Bangalore and Pune observed significant progress in acceptance of Smart home market. Panasonic, Sony, Samsung, LG Electronics Inc. Philips, XIAOMI, Google, Amazon, Mygate, Syska are the competitors in India. For Indian innovators, people, and business leaders, “Digital India” and “Make in India” together served as a significant call to action. Many companies in India are developing advanced products and technologies for the smart home industry.

Smart Homes were initially advertised mainly as homes with high-end security features. However, newer areas of the market are emerging, such as lighting systems, gas leakage alarms, smoke alarm systems, entertainment systems, and energy efficiency systems. As a result, Smart Homes not only offer improved protection, conveniences, and comfort to residents, but they also save large amounts of energy.

Companies can now compete not only on the functionality and performance of their services and products, but also on the knowledge generated by their use, thanks to the rise of smart and connected things. Sensor technologies, which are used in IoT products, make things "smart & intelligent". Comfort, entertainment, flexibility, and security are all incorporated into smart home technology devices, making solutions more convenient for them. Regulated lighting, heating, and other electronic appliances and household goods, such as the air conditioner, are among the items available. They can all be managed remotely from your own computer, smart phone or tablet.

Smart home application –

- **Security** - Many homeowners choose a complete CCTV surveillance device, which cover a larger area and record even in low-light conditions. A video door phone, on the other hand, is a more realistic solution for Indian homes. Remote door systems, such as the Trane electronic main door mortise lock, can be connected to these. Companies like Eureka Forbes offer video door camera at reasonable price.
- **Energy consumption** - The are endless possibilities, from integrated situation or mood lighting for your entertainment hubs to sensor-based LEDs that turn off when no one is in the building.

  Schneider Electric offers lighting control systems that can be accessed through a mobile device.

- **Atmosphere control -** Another choice for home automation is to use a mobile device to control the air conditioning or heating in home, even if no one is present. Before entering the home, one can switch off the air conditioner or turn on the heater.
- Additionally Smart Automation offers facilities that allow user to open or close curtains with the touch of a button from anywhere in the house. You may also use a remote to unlock the front gate or garage door from your vehicle. All of your home entertainment equipment can be synced so that you can access it from a single mobile app or remote. Automated systems may also be used to monitor Microwave Owens, refrigerator, and recirculating water systems.

What features do Indians seek in a smart home?

Though convenience is one of the factors, Indians value protection above all else in a smart home. The range of electronic gadgets aimed at improving a house's security includes video door control, motion detection cameras with night vision technology, digital locks, smart alarms, windows, and alarms. Intrusion cameras, fire and gas-leak detection are now used in smart homes.

Then there's the matter of ease, which is just another motivator. Smart homes are the definitive option at a time when people are constantly looking for easier ways to complete tasks. Cleaning homes, for example, is a physically demanding task that entails dusting and mopping. Cleaning has thankfully become a piece of cake, thanks to manufacturers now providing a wide range of robotic vacuum products.

Technology has revolutionised the way people consume content, from smart TVs and smart speakers to Audio Visual controls and game consoles. Smart entertainment systems have become commonplace in today's world, enabling users to schedule TV shows and change channels using voice commands. A lack of entertainment-based activities are particularly noticeable among youngsters and young couples.

Smart homes, which were once only available to India's upper crust, are now attracting buyers from the middle class. The idea of smart homes is spreading like wildfire as smart devices and home appliances become more affordable. As we move into 2021, more Indians are expected to consider giving their homes a smart twist by incorporating modern technology.

The most significant challenge that the smart home market faces is Privacy and security. Since almost everything in a smart home is linked to the internet, cyber-crime is a greater risk. Any unit in a smart home can easily communicate the owner's location and usage time. The consumer becomes absolutely vulnerable to cyber-attacks when they have this much data, putting their lives in trouble. In May 2018 Schneider electric India introduced Easergy p3 which was medium voltage guard relay that associates real-time analytics driven by IoT. Also apple have launched home-kit for i-Phone user to control individual smart devices such as garage parking garage opening system, lighting control, surveillance camera.

Smart Home systems have seen unprecedented demand in India in recent years, owing to increased concerns for a safe and secure living environment, particularly for safety functionalities and discrete monitoring for elderly people, especially in cities.

The growing demand for customer convenience, safety, and protection, as well as increased energy use, is driving the smart home market. Furthermore, factors such as improved lifestyles, increased spending power, and increased knowledge of smart automated systems have boosted the adoption of smart home products, resulting in the growth of the India smart home industry.

Factors driving the India smart home market include a rapidly growing IoT market, cost-cutting measures enabled by home automation systems, manufacturers expanding their product portfolios, and the growing importance of home monitoring from remote locations. As the demand for smart home devices grows, so does the risk of security and privacy breaches. The smart home market's growth is being suppressed by concerns about privacy and security breaches.

1.7. Advantages of Smart Home Innovations

Fortunately, we are living in the golden age of technological evolution. Smart home technology typically refers to any group of devices, appliances or systems connected to a common network that can be managed independently and remotely. Whenever home technology works together in one unit, it can also be more loosely pointed to as "connected home" or "intelligent home." For example, TVs, thermostats, smart lights, audio speakers (like Alexa), security surveillance cameras, door locks, other home gadgets are all connected to a common computer that can be controlled from your smartphone or tablet. Smart Home Automation gives us the ability to indulge ourselves in high-tech technology and convenience that was not possible before. As technological developments continue to grow, consumer home automation adoptions can make life easier and more enjoyable.

There are several practical benefits of using Smart Home Technology

1. **Remote control feature** - Don't underrate the ability to remotely control your house. User can give a command to home on an extremely hot day to get cooler just before you get home.
2. **The comfort and convenience** – This is a very big factor. Smart home technology helps users to monitor all home devices from a single place. Being able to maintain all devices connected with a single application at home is a big step forward for devices and home management. For this, all you need to do is learn how to use a single control system on your smartphone or tablet, and you can get into a multitude of functions of smart home.
3. **Adaptability & versatility** - New devices and appliances are designed to provide adaptability. When it comes to incorporating modern devices, appliances and other technologies, smart home systems appear to be remarkably flexible. No matter how state-of-the-art your appliances appear today, as time goes on, newer, more amazing models will be developed. In addition, it is possible that one will add to the machine suite as older ones are replaced.
4. **Better safety & security** - When users incorporate protection and monitoring features into the smart home network, it strengthen your home security. There are hundreds of options available. Home control devices, such as Security alarms system, door locks, motion detectors, surveillance cameras, and other

security appliances in your home. Biometric system, retina scanners and facial recognition technologies help in providing highly validated and authorised high-security systems.

5. **Improved quality of the Gadgets** - Smart homes functions will allow user to properly operate home appliances. Opening and closing doors and windows by means of voice assistance, music systems to soothe the atmosphere, automatic heating and lighting systems, refrigerators to order grocery stores, equipment to feed pets and equipment to relay warning alarms in the event of potential accidents. List is infinite
6. **Greatly improved energy efficiency** – Smart devices in smart homes allow users to monitor energy usage over time. It's possible to make your home more energy efficient, with the use of smart-home technology. For example, with a programmable smart thermostat that learns your schedule and temperature preferences, you can have more control over your home's heating and cooling system, and then recommend the best energy-efficient settings during the day. Lights and motorised shades can be programmed to switch to an evening mode when the sun sets, or when you enter or exit the room, the lights will turn on and off automatically, so you never have to worry about waste of energy.

1.8. Research Background

1.8.1. Big data: Big Role

Big data refers to the data that characterizes the 4V's - volume, variety, velocity and veracity. Managing such type of data requires added features in the conventional data management system. In smart home environment there is an immense role of big data and related technology. Smart home ecosystem comprises interconnected mesh of devices and wireless sensor network. Data generated by the smart home devices are thus big data. Database architecture such as Google Distributed File System (GDFS) and Hadoop are examples of big data management framework. Due to surge in the demand of connected environment during recent times, Big data has received a lot of attention in academia as well as in industry.

1.8.2. Big data collection & processing

The process of collecting quantitative and qualitative data on particular subject with an aim of measuring results or gaining actionable insights is known as data collection. To ensure that the data you collect is safe, consistent, and reliable, you need a clear method**.** When data is obtained and converted into usable information, it is called data processing. Data processing is usually conducted by a data scientist or a team of data scientists, and it is important that it is done correctly so that the final result, or data production, is not damaged. Data processing takes raw data and transforms it into a more readable format (graphs, records, etc.) so that machines can view it and organisations can use it. Data processing can also be further explained as data manipulation using a program. It entails the transformation of raw data into machine readable form, data flow through the CPU, memory, to output devices and finally formatting the output. Data processing covers immense use of computers to perform specified operations on data.

Data processing includes a variety of steps, such as:

- **Validation -** makes sure that the data provided is accurate and relevant.
- **Sorting -** arranging data in either in ascending or descending series and/or in separate sets
- **Summarization** – summing up the main points in short.

- **Aggregation** – a method of gathering information from various databases in order to prepare consolidated datasets for processing.
- **Analysis** – a process of surveying, cleansing, converting, and finding patterns in order to discover useful information, form conclusions, and support decision-making.
- **Reporting** – detailing or summarizing data, as well as computed information and its listing.
- **Classification** – refers to segmentation of data into multiple categories.

1.8.3. Difference between Analysis and Analytics

Data is viewed as a valuable asset in today's world. For instance, social media is generating voluminous data every day. Heavy use of smart phones, tablets and laptops have resulted into many fold growth of data which has resulted into data explosion. However, data will remain as data until it is utilized to generate information of business use. As defined by Merriam Webster, the separation of a whole into individual parts is known as analysis, whereas the science of logical analysis is known as analytics. Analysis focuses on the facts and figures of what has occurred in the past, analytics focuses on projecting the future or predicting a result. To put it differently, analysis rebuilds existing relevant information. The analytics then uses the processed data to forecast what could happen.

Data analysis is the process of studying a given data set in great detail, splitting it into small components, and studying in relation to one another.

Data analytics, on the other hand, is a broader concept that refers to a discipline that comprises all aspects of data processing, containing data collection, cleaning, organisation, storage, administration, and analysis using advanced tools and techniques. In other words, data analysis is a process or system, while data analytics is a broad field. It is the science or perceptive method that an analyst employs to identify problems and analyse data in the most effective manner.

Data analysis is the research, refinement, transformation, and training of historical data in order to obtain useful knowledge, draw conclusions, and make decisions. Data analytics is the process of gaining better insight and designing better strategies by combining data, machine learning techniques, statistical analysis, and computer-based patterns. It is the method of analysing and instigating past data into practice.

1.8.4. Big data Analytics

With millions of things and devices connected in an IoT-based smart home, a massive amount of data is generated. These large data sets are managed using big data framework which is then analysed using big data analytics. This helps to understand the contextual relationships and patterns that affect Smart-home owners. IoT is driving big data analytics for making real-time decisions. (Ravindra Savaram, 2018).

To assist for better utilisation, the data can be used by various agencies

- **Device venders:** to understand requirements of better, safe and secure & develop the devices accordingly
- **User:** for better engineering practices so as to make maximum usage while maintaining privacy of users data and Home security
- **Authorities:** to make/amend appropriate laws to ensure better use of protection
- **Applications vendors:** to develop better tools for improved data visualising and supported analytics. This can be further enhanced using AI Algorithms.

Big data analytics aids in the prediction and resolution of problems before they occur. Big data and IoT work together to shift asset reporting from passive to proactive. We need to understand the relation between big data analytics and data collected from smart Devices. They must provide useful services or tools while also collecting necessary information. It is not enough to simply collect data. It must be analysed and processed in order to generate insights, which must then be translated into actionable steps that can improve security operations. A proactive approach is required, which entails detecting problems early on and devising solutions. By designing analytics solutions with major risks in mind, most issues related to safety and security, as well as any other major issues, can be avoided.

Currently a lot of interest in using information technology (IT) to collect big data in networked communities or in domestic environments, which are commonly referred to as smart homes and/or ambient assisted living, in order to increase the volume, variety, and velocity of data and information (Big Data, Smart Homes and Ambient Assisted Living, V. Vimarlund, 2014). Service providers and research organisations are concentrating on how to generate, combine, evaluate, and effectively use big data from different and distributed sources in order to provide services at home. Big data is projected to radically change the delivery of smart homes and ambient assisted living facilities, as well as the management and economic aspects of safe home services and improve the quality of life.

Chakravorty A (2013) stated that that the information provided by smart homes is sensitive, and that privacy concerns are not always flawless. They also explore the types of data that are obtained, stored, and exchanged, as well as the importance of linking data from various sources. They also talk about how sensors can transmit data, how networks can be secured, and how confidentiality needs to be strengthened in order to protect sensitive data. The data's integrity and the reliability of the individuals should be protected. Further how data is stored and what measures are required to protect privacy, how to maintain probability properties and data consistency, and how access to the system can be ensured through proper authentication and authorization of users are all topics that have recently been discussed in recent publications.

Challenges in IoT- based system utilizing big data analytics

- **Data storing & managing** – In a smart home ecosystem, data generated by the connected devices grows at an exponential pace, and the storage of this big data is a challenge. Therefore, storing and managing such a large volume of data is an issue. To collect, save, and manage this data, some processes and frameworks must be designed.
- **Data Reliability** - Connected devices are capable of sensing, interacting, exchanging information, and performing analyses for a variety of applications. Data assemble methods must effectively deploy scale and conditions of integrity with certain common procedure and guidelines, as these devices ensure users do not share their data indefinitely.
- **Power consumption -** For the smooth and continuous running of IoT operations, internet-enabled devices should be linked to an endless power

supply. As most of the devices used in smart home ecosystem are constrained device, they have limited energy, memory and processing ability. Though Edge computing and roll out of 5G network will improve the efficiency of smart home working in future.

- **Data visualization** – Data generated by smart home devices are heterogeneous in nature. Since data is combination of structured, unstructured, and semi-structured and are in various formats, it is difficult to visualise. Data must be prepared for better visualisation and summarization in order to make correct and timely decisions and increasing the business productivity**.**
- **Privacy and ethics -** Each smart object in a globally connected network is an IoT device, which is primarily used by any users or by a systems; this raises concerns about privacy and data leakage. As a result, the sensitive data should be kept private and confidential, as it includes sensitive information about users. **(Mantripajit kaur, 2016)**

Data analytics for security can work wonders and significantly improve an ability to respond to attacks and data breaches. Better identification, risk control, reporting, and automation can all be supported using big data analytics. Machine learning algorithms can aid in the analysis and prediction of threat trends.

1.9. Significance of the study

The interest and need for new technology is growing on a daily basis. Fascination with creativity, combined with the need for convenience, has given rise to the concepts, creation and output of these new technologies. One technology in particular that has drawn tremendous attention is smart home technology. With smart home technology, the home can be designed for comfort, protection and accessibility by being able to monitor various parts of the home using a smartphone or remote control. A smart home as a place to live in computing and Information technology has been applied via networking inside and outside the home. This solution can then adapt to the needs of everyone inside a home, and the service may provide functions that can be used to promote convenience, comfort, protection or entertainment. Smart technology can be used to monitor TV, lighting, temperature, various sets of appliances (such as a coffee machine or air conditioner) and more.

Although the Smart home automation will make our lives easier, it will also introduce new hazards. Users may face additional opportunities as well as risks, as with any other new advancement. Security and privacy are major problems for IoT technology and its widespread adoption, according to a number of academic study publications.

By surveying a sample of Home users about their worries and opinions on the matter, this study seeks to address the issue of smart home user’s security and privacy.

The study will show how current methods of IoT security is insufficient, and that there are several flaws and dangers to end users. The study will explore the obstacles and give an analysis for future research effort in order to enable a more informed decision.

This research will not make any use of data analytics tools or related technology for the same. The emphasis is on privacy and security of smart home environments which are using big data analytics. For sustainable smart home, use of analytics over big data (generated by smart home ecosystem) is a must. This portion of service is managed by the smart home service providers/vendors.

1.9.1. Need of the study

With India's fast-changing lifestyle, there is a tremendous need for home automation solutions. Some of the key factors before implementing home automation solutions are protection, safety, convenience, comfort, energy savings, etc. In smart city projects which are being implemented by central government or integrated townships, the connected home is a part of an ecosystem consisting of various city assets such as utilities, defence, transportation, health care, public safety, environmental services, etc. By being a part of a broader ecosystem, smart and connected homes will help the entire ecosystem function more effectively and efficiently.

1.9.2. Motivation

Effective Protection & Security are key drivers for adoption of Smart home technology. The provision of technology, techniques, practices, and infrastructure that mitigates unacceptable risks, systems that are sufficiently secure enable stakeholders to benefit from facilities and experiences that would otherwise be intolerably harmful. The problem is the need to determine if there is an adequate protection, unacceptable threats to the related stakeholders. This includes a clear understanding of vital principles such as safety, confidentiality, integrity, availability, transparency, etc.; awareness of risks, vulnerabilities, and controls; ability to understand, enforce, use, and sustain security controls; and ability to make trade-offs that align security and privacy with business imperatives: e.g. user privacy vs. ad-supported privacy. Although attempts are being made to research and protect home environments, there is a substantial gap in the skills, experience, awareness and services available to home users and families. Despite some initial work to explore this domain, much needs to be done. Securing home devices, utilities and data is becoming increasingly difficult and necessary. Though home users are not as glamorous as many companies, they are both commonplace and vulnerable to multiple attacks. Initial work to investigate the protection and privacy of home computer users has demonstrated the significance of this area, and yet much more needs to be done to resolve the scale and complexity of security and privacy challenges. A study in India reveals common threats and attacks against home users includes viruses, malware, spyware, key loggers, identity theft, privacy violations, and phishing to name a few. It seems the best practise to mitigate viruses in the home environment is needed. Home users have a limited skilled resources, ability and knowledge to defend themselves effectively from the threats that aim to directly harm them. In today's highly globalized society, digital communications security relies on the security of all the different devices linked through internet. If not well-protected, home networks can be exploited by attackers and used to target critical infrastructure like communication, utilities like banking and healthcare that are highly dependent on the secure functioning of cyberspace. Recognizing the need for better security for home computer users, a key approach for improving home security practises focuses on increasing wakefulness. Recent events show that home users remain vulnerable to several attacks that have facilitated unsafe practises and choices to ignore security advice. In the context of this, the research community has realised the need for further exploration pathways for effective ways to secure home users. Though various approaches have been recommended, rising number of accidents and a strong lack of effectiveness in the protection of home users have inspired this research into the essence of the problem of protecting home users. In order to build more suitable and efficient security solutions, it is assumed that safe and sound security systems in the home must be based on an actual scientific and grounded understanding of home users, the context in which they work, and how they make data security decisions.

1.9.3. Benefits of privacy and security in Smart home

Charlie Wilson (2017) in his national survey explained the potential benefits of Smart home environment. Home owners are looking for possible benefits of smart home technology in saving electricity, time, money, managing overall house hold resources and complete home security thereby making domestic life self-driven and effortless.

Some of the listed benefits of privacy and security in smart home is given below:

- Remote access and management of smart home devices.
- Instant access to information by enabling smart home users to track their home on demand.

- Tracking and accessing real time information related to any aspects of smart home ecosystem.
- Peace of mind through fully secured smart home surveillance systems.
- Smart security system has direct impact on people's safety.
- Convenience in protecting home and belongings.
- Enable consumers to respond quickly in an unexpected events
- In proactively save home from any kind of malicious danger/ destruction
- Monitoring facility for children, differently able house member and old aged people using devices like video monitoring, motion detection, etc.
- Customization of personal preferences such as heat, light or ambience.
- Improved safety features compared to traditional devices.
- Improvement in quality of life.
- Provides self-protection.
- Facilitating assisted living related to health issues.

1.10. Chapter Structure/Scheme/Thesis outline

These chapters are the building blocks required to obtain a deep understanding of the issues at stake and to serve as the basis for the rest of the thesis.

1 **Introduction**

This chapter will provide the context and background details on the subject of study. Research problems are addressed and the purpose of this research is discussed.

2 **Literature Review**

This chapter critically summarises and discusses the related literature on the research topic. The chapter sets out the Smart home technology and its effect on Day to day life of the user. The chapter then addresses the related IoT enabling technologies. The advantages and value of the IoT is illustrated. Security threats are explored in great detail. Privacy, governance and legal issues are finally discussed.

3 **Research Methodology**

This chapter describes the available methodological approaches. The philosophy, methodology and study methods are presented, and then the choice of study is justified. The data collection, population and sampling method is discussed in detail. Ethical issues have been clarified. Finally, the drawbacks of the methodological approach and the lessons learned are illustrated.

4 **Data Analysis & Interpretation**

This chapter presents the analysis and findings of the data collected during the research. The qualitative research is analysed followed by the themes and finally proposition of the framework.

5 **Findings Conclusion & Suggestions**

The dissertation concludes with this chapter. Answers to the research questions are presented. Proposed conceptual framework Safe@SmartHome using, big data Analytics is explained. Key results from the study are discussed. Finally, attention is given to weaknesses and future prospective works.

CHAPTER 2
LITRATURE REVIEW

2. Introduction

This chapter presents the conceptual and empirical basis of the study. It lays the foundation for the thesis. In this chapter, smart technology is explained, with further guidance through the concept of smart home technology. Security for smart home technology is exhaustively elaborated and investigated.

2.1. Literature review process

Secondary data was discovered and gathered utilising EBSCO's online database service, as well as Google Scholar, IEEE, Emerald, and Scopus. Academic materials including scientific publications, conference papers, and journal articles are available through these sites. The secondary data collecting process began with a keyword search for related literature. The keywords were picked based on the subject and research question, and included topics such as smart home technology, dangers, and vulnerabilities. Smart home technology risks, smart home technology security, Internet of Things security, and home automation security were among the terms utilised.

In order to have a better knowledge of the history and evolution of these technologies, terms like "Smart home technology" and "Internet of Things" were used in the search string. As a consequence, substantial materials were obtained and rigorous study was conducted. (Oates 2006) outlines a literature review as a two part process, the first of which is searching the literature for the issue area to be investigated. The materials required for this phase of the way should have been identified during the literature review phase of the process. The articles were then gathered and read. Articles that were deemed to be too old or irrelevant were eliminated, and those that looked to be related to the issue were preserved separately for further examination. The publications that were deemed relevant were picked based on a number of variables, including their age. If the article was older than 12-15 years, it was considered obsolete, unless it included data that was unaffected by its age. Another consideration was that it should include knowledge on the technology in issue, which is smart home new tech, as well as information of related technologies such as home automation, the Internet of Things, or ambient intelligence, as well as security-related research. Another consideration was that it should include knowledge on the technology in issue, which is smart home new tech, as well as information of related technologies such like home automation, the IoT, or artificial intelligence, as well as security-related research.

2.2. Smart Technology

The evolution and advancement of our everyday technologies has resulted in smart technology and smart settings. New and better technologies are developed and enhanced as a result of public interest, demand, and convenience. The most prevalent definition of smart technology is that it connects devices to make life easier. (Cook, 2012).

The focus and the need for what smart technology can do for one varies depending on the person and environment, such as the need to increase or ensure safety, gain a better understanding of energy consumption, or automate daily tasks that are common in one's surroundings, all of which can be accomplished using smart technology. (Cook, 2012; Robles, Kim, Cook & Das, 2010).

(Worden, Bullough and Haywood 2003) Smart technology is described as a piece of equipment that is aware of its surroundings and can respond to them. The authors go on to say that a smart technology must have various components in order to achieve these two qualities. Sensors and measuring systems are required for technology to be aware of its surroundings. Actuators are required for the technology to react to the information that it has detected or measured from its local environment in order to accomplish the function that is of interest.

The technology is almost willing to perform smart operations, but the scientists add that *"advanced signal processing methods and control techniques"* are also necessary for these two processes to operate together. This is especially important if the technology wishes to execute many activities at once which is based on the data the system collects from the surrounding environment. Any smart environment system requires data from the environment in order to work effectively. The system must be able to acquire sensory inputs from its surroundings and utilise that data to perform an action. (Cook & Das, 2004).

Devices must share information in order for smart technology to communicate. This is known as machine to machine communication (M2M), where intelligent or smart gadgets may interact with each other without the need for human interaction. (Chen & Li, 2012).

M2M is required for smart objects to be able to communicate, which is then utilised to obtain information and control the surroundings across a wired or wireless network. (Hui, Sherratt & Sánchez, 2016).

An array of sensors and actuators must be installed in order to regulate the environment. Sensors are devices that interpret the environment and can transform those interpretations into signals that can subsequently be measured. A movement in a room, for example, may be detected by the sensor. Actuators then analyse the data received from the sensors, depending on that information, either close circuits or modify the strength of the electric load, such as turning on a light that was previously turned off. (Domingues, Carreira, Vieira & Kastner, 2016).

2.3. Communication Technologies

In order for the devices to interact, they use a collection of networking and protocols called as Short-Range Wireless (SRW), which comprises protocols and platforms including Zigbee, Bluetooth, and Thread. (Hjorth & Torbensen, 2012). There are many protocols today which can be used, here follows a brief description of some of the common ones.

2.3.1. Zigbee

The Zigbee Association was founded in 2002 and is made up of a consortium of firms that combine to develop standards, certification programmes, and tools for the IoT market. Their standards, certification, and tools are aimed at assisting the advancement of low-power and wireless IoT solutions. They also want to provide a comprehensive range of security solutions to enable the creation and maintenance of safety in more than one billion Zigbee-enabled devices throughout the world. (Zigbee, 2017e).

In early 2007, researchers (Baronti, Pillai, Chook, Chessa, Gotta, and Hu 2007) forecasted that the Zigbee protocol would be used in a wide range of appliances in the forthcoming days.

2.3.2. Z-Wave

Z-Wave is a wireless technology that utilizes a mesh network structure to communicate. Because each device acts as a signal transmitter, the devices that are linked to the Z-Wave protocol get stronger as more devices are connected (ZWave, 2017).

The Z-Wave Collaboration, which was founded in 2005, devised the communication technology Z-Wave. It is made up of a number of firms and industry professionals that are working to develop Z-Wave for smart homes and commercial applications. (Z-Wave Alliance, 2017b).

Z-Wave is the most widely used based home automation system. It has over 1700 approved products available all around the world. Because of its qualities such as flexibility and security, Z-wave is the most extensively utilised and trustworthy technology.

2.3.3. Wi-Fi

The Wi-Fi alliance is a group of firms that supply the Wi-Fi tech, which is a wireless local area network. The purpose of Wi-Fi is to allow devices to connect and communicate over the internet. (Wi-Fi, 2017a).

Wi-Fi Home Design is a new proposal by the Wi-Fi Alliance to join the smart home industry by allowing the wireless network to be used in the blueprint designs. The alliance will give instructions on how to set up a wireless network in a home so that a strong connection may be established everywhere in and around the house, such as in a garage or on a porch. (Williams, 2017).

The Wi-Fi Home Design will give instructions to the building industry, including guidelines for how hotspots should be set up to maximise wireless connections, as well as standards for smart appliance incorporation. (Wi-Fi, 2017b).

2.3.4. Radio-Frequency Identification(RFID)

RFID is one of the most essential instruments in IoT for resolving item identification concerns in a cost-effective way. RFID's primary components are the tag, reader, antenna, access controller, software, and server.

2.3.5. Wireless sensor Network (WSN)

A wireless Sensor network (WSN) is a collection of geographically dispersed independent devices that use sensors to control physical or ecological factors such as temperature, sound, vibration, pressure, or motion at many places. WSN may be utilised in a variety of applications including army, Home safety, healthcare, field monitoring, manufacturing, and forest fire detection.

2.3.6. Bluetooth

Bluetooth offers wireless connectivity by providing connection through radio waves. A product which is using Bluetooth will come with a computer chip, which in turn can be used to connect the product to another device or software (Bluetooth, 2017). This is a cost-effective approach because no regular wiring is needed.

The Bluetooth technology and the devices which can use it are susceptible to several attacks, such as Denial-of-Service (DoS), eavesdropping, and message modification. Bluetooth technologies may potentially be risked by flaws in their own technology, as a result of their specification and implementation. An attacker can with these vulnerabilities access sensitive information, or gain access to the connected devices or network which they are operating on (Padgette, 2017).

2.3.7. Thread

Tread Group introduced Thread to the market in 2016. As a communication technology, it is gaining popularity and is endorsed by some of the industry's largest names, including Apple, Samsung. This communication system is designed to be unique in terms of smart home device interoperability, protection, energy, and architecture. Thread is a low-power mesh networking protocol that can connect devices to devices as well as devices to the cloud. It is based on the IEEE standard 802.15 and has no single point of failure (Saeedreza Arab, 2018).

2.4. Different areas to apply and use smart technology

Other than the house, smart technology may be used to enhance functionality and provide convenience in a variety of industries and places. Smart technology can be used in the workplace. (Rottondi, Duchon, Koss, Palamarciuc, Pití, Verticale & Schätz, 2015), warehouses (Zebra, 2017), health care (Sprint, Cook, Fritz & Schmitter-Edgecombe, 2016), elder care (Lühr, West & Venkatesh, 2007), Education Institutes, playgroup (Srivastava, Muntz & Potkonjak, 2001), and many more.

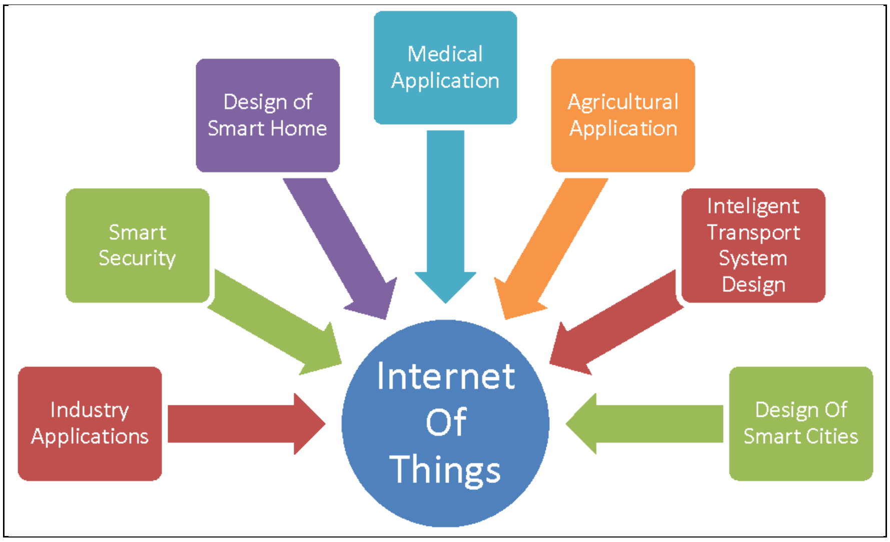


Figure 2.1 IoT Applications

Source: https://www.semanticscholar.org/paper/Security-and-Privacy-Consideration-for-Internet-of-Desai-Upadhyay/dd05e2c2060dd1181bb4de45c09b43c6680173da/figure/1

2.4.1. Smart health care / Medical applications

Chen, Campo, Estève, and Fourniols (2009) have conducted research on the use of smart technology in the elder and health care sectors and discovered that the early ideas for utilising technology in the house to assist with health services were centred on the necessity to transfer health data from the house to data repository. Different equipments such as motion sensors, hypertension, heartbeat, and body temperature measuring devices needs to be installed in the house, which would then be attached through a network. The data collected is relayed to the intended computer server at a health care institution where it will be viewed and analysed. Data will be captured at the centre and entered into software which then perform analysis, track trends in the data using algorithms and alert the appropriate personnel in the event of an adverse incident. Someone who need senior or health care can stay at home, and their health pattern may be observed, thanks to the connected house providing data to the health institution.

Chan et al. (2009) it was also discovered that, as technology advances and health-care prices rise, having a smart supported living in the house rather than a health-care centre will save resources. They do, however, stress that privacy and confidentiality must be considered, as well as ethical and legal considerations around how individuals would be watched in these houses.

Patients' privacy and security must be preserved while using tele-home care systems, according to previous studies. The study also found Demiris (2004) that integrating smarter systems with services that can also be utilised at home can improve quality, such as patient care at home. Caretakers can improve the quality of care through regularly monitoring their patients, have expanded access to different care facilities as well as visit frequency, there is the possibility of early detection and treatment when needed, and they can have a higher involvement in their patients and their care process, to name a few advantages. Patients' capacity may be strengthened by offering them more information, autonomy, and control, as well as a sense of satisfaction with the care services provided to them.

2.4.2. Building automation systems / Smart Home

A building automation solution can be used to control functions within a structure. This type of system will link gadgets that monitor and regulate a technologically enhanced environment. Heating, illumination, security systems, and other functions may be controlled in a variety of settings, including businesses, warehouses, and residences. (Domingues et al., 2016).

When designing automation systems, it is necessary to decide whether the system will be wired or wireless. The advantage of employing a wireless system is the mobility and flexibility it provides, as well as the ability to eliminate wiring issues. (Cook & Das, 2004). Having a consistent home automation system would be ideal to allow for system compatibility, however due to the variety of products, a single solution is unachievable. This is mostly owing to devices including large number of varied type of sensors and actuators, each with its own set of needs.

2.4.3. Smart grids and Industry

Another notion that has been considered in recent study on smart technologies is the smart grid, which is the measurement and awareness of energy usage in a smart fashion. Electrical networks that utilise smart functions to detect and measure energy products are known as smart grids. These could be used for larger operations, which including energy plants, to generate and distribute energy in a fast and efficient manner, but they may also be used for smaller concerns, such as measuring one's household power use. As a result, smart grid technology may be well-integrated and applied in a smart home. (Kabalci, 2016).

Metering for energy use, as well as smart grids, have become increasingly widely used in China in recent years. (Zhou, Yang & Shen, 2017).

Homeowners in Kunshan, China, had their power use tracked using smart grids. They discovered that using smart grids to measure and analyse electricity usage data can provide significant information for smart power decision-making. Further study has been carried out combining the Industry 4.0 strategy with smart living. A study by Batista, Melício and Mendes (2017) recommended a smart home and smart living paradigm based on the Industry 4.0 Interconnected Things paradigm, which resulted in benefits such as the ability to connect different technology solutions in the same architecture, increased security advantages, better obtainability, and faster recovery procedures during failure.

2.4.4. Smart cities

The idea of smart cities has gained a lot of traction in recent years, with a slew of initiatives springing up in towns and nations all over the globe. With the increased use of smart technology in many regions of cities and nations, there has been a growth in interest in bigger notions such as smart towns and cities. A smart communities are defined (Li, Lu, Liang, Shen, Chen, and Lin 2011) as an environment that comprises of residences that are connected to networks and have smart technology installed. The smart community also was regarded as virtual, and it should be restricted to a specified geographic region. A smart community, according to the authors, should include three key domains: a residential domain, a community domain, and a commercial services domain. A home network is set up in the home domain, which can include one or more smart technologies, such as a physical security or a health-care system.

The community sector is made up of all the gates in the community's individual residences, which together comprise the smart community's center. All of the data collected by these gateways and connected home systems is sent to a community communication centre, where it may be analysed to get a greater understanding of the community's surroundings.

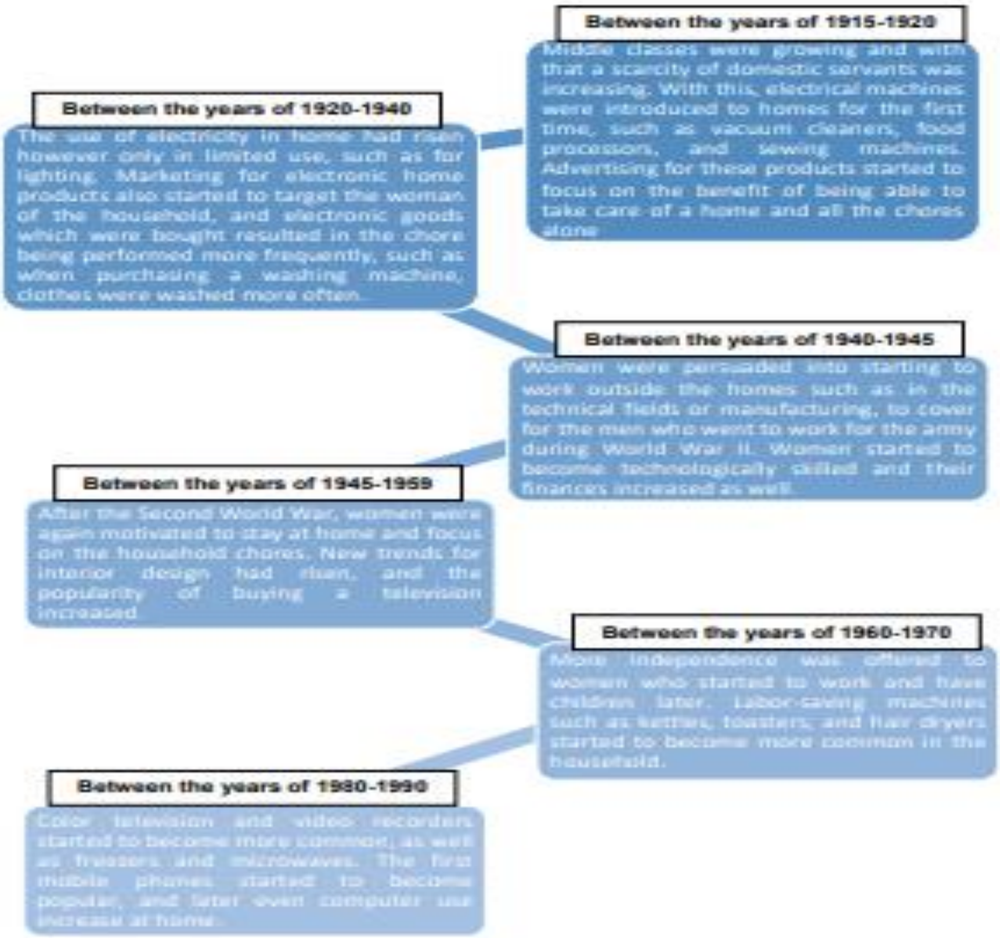
Finally, the utility sector will provide a call centre for the smart community. The call centre will receive information from the community domain that has been verified and may be regarded valuable or relevant to the public. This call centre would be run by a reputable host, such as a police department, who would be in charge of managing the information and, in the event of an emergency, contacting the appropriate authorities (Li et al., 2011).

Mosannenzadeh, Bisello, Vaccaro, D'Alonzo, Hunter, and Vettorato (2017) According to their findings, there is a link and relationship between the phrases smart energy town, smart environment, and sustainable city, with the energy system being a key component, region, sub-system, or element of a smart city. In certain circumstances, the energy system is even regarded as the smart city's heart. Mosannenzadeh et al. (2017) As a result, it's critical to look into and explore smart energy systems in order to expand on the notion of smart cities. There are several sites that forecast the future success and expansion of smart technology in the house, and prior research has also advised technology companies to guarantee that the technology is trustworthy and that privacy is protected. As a result, people will have an easier time adopting and trusting this technology and incorporating it into their homes. (Friedewald, Vildjiounaite, Punie & Wright, 2007).

2.5. History of smart home technology

Smart home technology has a long history. It's crucial to analyse how technology and humans have evolved together when it comes to recognising the spark of smart home technologies. The introduction of electricity in houses at the turn of the twentieth century was a significant step toward the development of smart home technologies. This includes everything. Information technology started the creation of smart home technology around the end of the nineteenth century, allowing the technology to exist and promote. (Harper, 2003).

Harper (2003) has made a past analysis of the growth and background of smart home technology which contains the following important groundings:



Between the years of 1915-1920

Middle classes were growing and with that a scarcity of domestic servants was increasing. With this, electrical machines were introduced to homes for the first time, such as vacuum cleaners, food processors, and sewing machines. Advertising for these products started to focus on the benefit of being able to take care of a home and all the chores alone

Between the years of 1920-1940

The use of electricity in home had risen however only in limited use, such as for lighting. Marketing for electronic home products also started to target the woman of the household, and electronic goods which were bought resulted in the chore being performed more frequently, such as when purchasing a washing machine, clothes were washed more often.

Between the years of 1940-1945

Women were persuaded into starting to work outside the homes such as in the technical fields or manufacturing, to cover for the men who went to work for the army during World War II. Women started to become technologically skilled and their finances increased as well.

Between the years of 1945-1959

After the Second World War, women were again motivated to stay at home and focus on the household chores. New trends for interior design had risen, and the popularity of buying a television increased

Between the years of 1960-1970

More independence was offered to women who started to work and have children later. Labor-saving machines such as kettles, toasters, and hair dryers started to become more common in the household.

Between the years of 1980-1990

Color television and video recorders started to become more common, as well as freezers and microwaves. The first mobile phones started to become popular, and later even computer use increase at home.

Figure 2.2 History of Smart home Technology

All of these advancements and technologies have paved the way for smart home technology to emerge. Electronic products were created to save time or energy, and households began to become increasingly linked. Over the years, marketing has placed a strong emphasis on home ease and efficiency.

Many new related technologies are established as a result of these technical advancements, with inspiration from the preceding ones. The goal is to make these technologies more helpful and convenient. Artificial intelligence is one example, which is closely tied to smart technology. Artificial intelligence tries to build a smart environment by utilising sensors and then modifying the environment finding of this research. (Cook, Augusto & Jakkula, 2009).

2.6. What does a smart home system consist of?

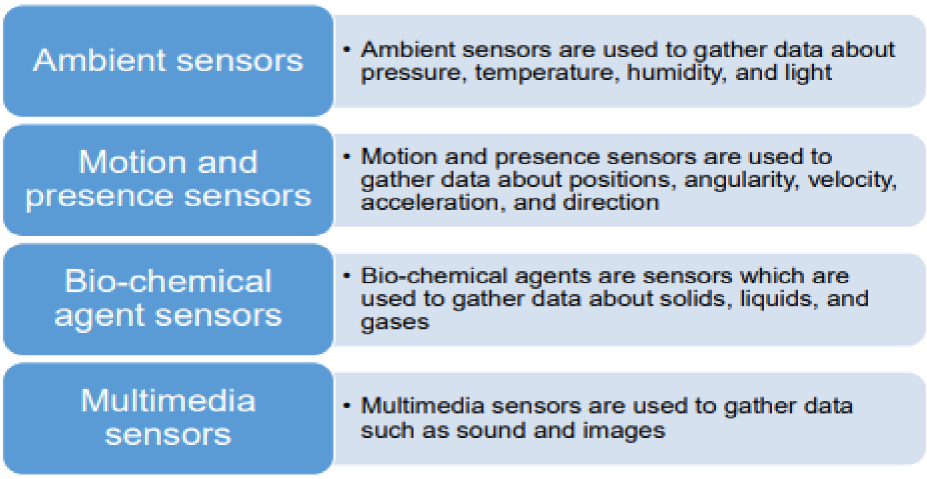
The correct components must be assembled in order to have and use a system to control various operations of the house for convenience, privacy, or just pleasure. To allow information to be exchanged from and to the system, a variety of electrical components, as well as a mobile and wireless systems, are necessary, according to (Suryadevara and Mukhopadhyay 2015).

That data needs to be analysed, with the outcome being the activation or deactivation of a function, such as turning on the lights because a human entered the room and a sensor gets triggered. Sensors and other physical components in the smart environment collect data and send it to the home monitoring command system. The system is interconnected and enables for the collection and processing of data. The environment can be influenced based on the pattern or demand derived from this data (Suryadevara & Mukhopadhyay, 2015).

2.6.1. First element – physical

The physical components are installed in an environment that will be managed by a smart system. It's critical that the equipment are strategically arranged so that they too can collect the data they require in the most efficient way possible.

Sensors and actuators have been the most frequent physical components. Sensors are used to gather data about the environment. Sensors of many types can be used to collect various types of data. Based on arena study, Suryadevara & Mukhopadhyay (2015) divided sensors into four categories:



Ambient sensors

- Ambient sensors are used to gather data about pressure, temperature, humidity, and light

Motion and presence sensors

- Motion and presence sensors are used to gather data about positions, angularity, velocity, acceleration, and direction

Bio-chemical agent sensors

- Bio-chemical agents are sensors which are used to gather data about solids, liquids, and gases

Multimedia sensors

- Multimedia sensors are used to gather data such as sound and images

Figure 2.3 - four categories of sensors

2.6.2. Second element – Communication

The communication component is the second crucial component of a smart home system. Information must be exchanged and processed between sensors, actuators, and the whole system, which necessitates communication. The communication method can be wired or wireless, and each has its own set of benefits and drawbacks. A Common example of communication systems used for smart home systems is Wi-Fi, Z-Wave and Zigbee (Suryadevara & Mukhopadhyay, 2015).

2.6.3. Third element – Data processing

The final component required to complete the home automation system is a method for the system to process the data it collects. Data is acquired from the sensors, which should then be utilised to complete a task correctly. The major goals of data processing are there to provide compatibility, flexibility, resilience, and real-time data processing. (Suryadevara & Mukhopadhyay, 2015).

2.7. Internet of Things (IoT)

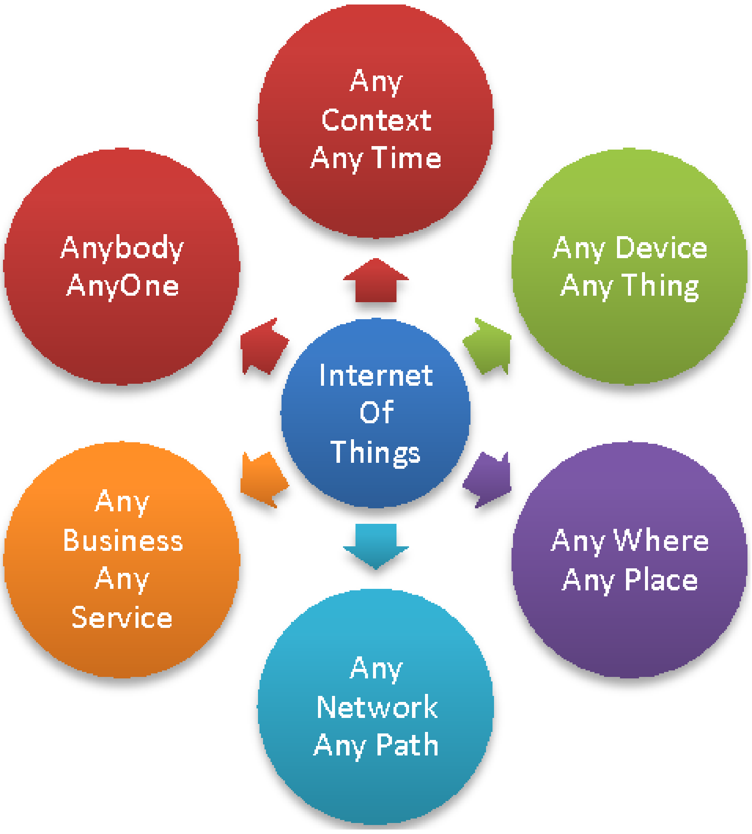


Figure 2.4 Definition of IoT

Source: https://www.semanticscholar.org/paper/Security-and-Privacy-Consideration-for-Internet-of-Desai-Upadhyay/dd05e2c2060dd1181bb4de45c09b43c6680173da/figure/1

The Internet of Things (IoT) is also another topic that is strongly tied to smart home technologies. Internet of Things is described by (Suresh, Daniel, Parthasarathy and Aswathy 2014) as Human beings, computers, and things being connected through internet. All of the gadgets we need and utilise in our daily lives may be controlled by IoT.

Batista, Melício, and Mendes (2017) various entities try to associate terminology like IoT with smart technology, like referred to IoT as the Network of Sensors and Actuators, which are the two main components of smart technology. The possibility to incorporate IoT and smart features is rising as the number of microprocessors in everyday use devices grows. It will become easier to connect a growing number of gadgets to provide convenience and "smartness." (Cook & Das, 2004).

Fortino and Trunfio (2014) describe One of the primary components of the Internet of Things is smart things. According to the authors, a smart object is a commonplace thing or gadget made up of hardware components that can process tasks, communicate, and be aware of their surroundings through the use of sensors and actuators. With the aid of the sensor, these items may control or respond to the surroundings. In turn, these objects can control or react to the environment with the help of the sensors and actuators which they are equipped with. Further on the authors define Smart environments are those in which smart items may connect and communicate with one another.

Stojkoska and Trivodaliev (2017) further explain IoT as smart appliances or objects being intersected and forming a network on its.

Kshetri (2017) China's IoT development is among the most advanced among developing nations, according to the report. Many influential factors have enabled China's development to grow at such a rapid pace. In China, sensors and RFID are already widely used in goods, and the cost of these components continues to fall.

The author also cited various impediments to China's progress in the IoT, including a lack of software development expertise, a lack of quality in specific areas, and low regulatory obstacles for privacy and security. According to the author, as a result of all of these relevant variables coming together, China will have more incentives and chances to embrace IoT. In today's world, the Internet of Things (IoT) is both an opportunity and a challenge. The IoT refers to devices that link living and non-living objects over the internet. IoT is a system that enables physical objects to associate with digital devices. The IoT can also be defined as a global network that enables communication between things-to-things (T2T), humans-to-humans (H2H), and humans-to-things (H2T) via the internet. The goal of the IoT is to allow things/objects to connect to anything, at anytime, anywhere, with anyone, and with any service. Computers, smart phones, and tablets are the most common devices that can connect to the internet. However, everything in the home can now be done online, from gas to vending machines to cars that can talk and send messages to other gadgets. This amount of hyper-connectivity is unprecedented.

Basic building block of IoT

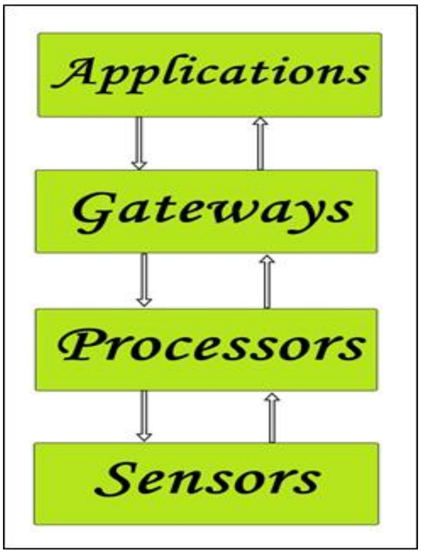


Figure 2.5 Basic building block of IoT

Source: https://www.weblineindia.com/blog/building-blocks-of-iot/

- **Applications**
  - One endpoint of an IoT environment is applications that are required for the proper usage of all acquired facts.
  - The cloud-based applications are responsible of providing the data collected a significant meaning. Users control applications, which aid as a distribution point for specific facilities.
  - Home automation apps, security systems, and industrial automation apps are examples of applications.
- **Gateways**
  - Gateways provides channelling handled data and give directions to the appropriate destinations for appropriate use.
  - Further, a gateway assists data connection among two points. It allows data to retrieve through a system. All IoT system that needs to connect requires internet.
  - Network gateways contain things like Local Area Networks, Wide Area Networks, and Personal Area Networks.
- **Processors**

    - Processors are considered as head of IoT system. Its prime duty is to process the data composed via sensors in order to extract valuable information from the enormous amounts of data acquired. In a nutshell, it provides insight to the data.
    - Processors are primarily real-time devices that can be easily manipulated by software. They are also in charge of data security, which includes data encryption and decryption.
    - Embedded hardware devices, such as microcontrollers, process data because they have processors attached to them.
- **Sensors**
    - Sensors are the IoT systems front ends. They are considered as the system's presumed "Things". Their prime function is to collect data from the surroundings using sensors or to communicate data to the environment using actuators.
    - These should be separately recognisable devices with particular IP address so as to be easily recognized on a wide network.
    - These essentially active and must be capable to generating the data. These can either function independently or are programmed by a user to fit their individual requirements.
    - Gas detection, Flood sensors, humidity sensors, are different specimens of sensors.

2.7.1. Typical IoT Ecosystem

The Internet of Things environment is difficult to describe. Due to the vastness and evolving possibilities, as well as the rapidity with which it is spreading across the entire market, it is also difficult to capture its proper picture. The IoT ecosystem, on the other hand, is a set of different types of devices that sense and analyse data and interact with one another over networks. The consumer in the IoT ecosystem uses smart devices such as smartphones, tablets, sensors, and other devices to send commands or requests for information to devices over networks. After being evaluated, the system responds and executes the command to send information back to the user through networks.

IoT ecosystem following steps (Avirup Dasgupta, 2019)

- Physical objects which are equipped with electronic devices, software, sensors, and actuators, powered by batteries, electricity, or RFID. Objects gather raw information from their surroundings. Every item has a distinct IP-address as well as differing computing resources and configurations.
- The application processes the data gathered from the objects.
- Data is transmitted using various communications technologies such as WI-FI, Bluetooth, Zigbee, near field Communication, cellular (2G/3G/4G/5G) and low-powered Wide area Network.
- The application gathers data in real time from various sources in order to store, manipulate, and evaluate it on a calculating platform.
- Rigorous analytics are used to extract insights from the collected data.

2.8. Definition of Smart home

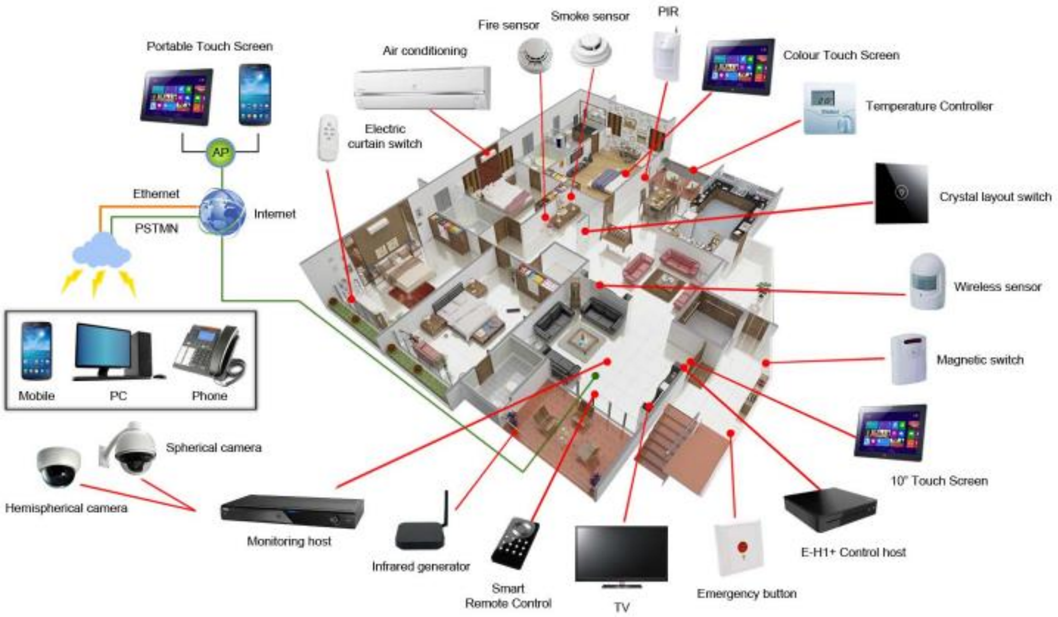


Figure 2.6 Definition of Smart home

Source: https://habr.com/ru/company/iridiummobile/blog/387809/

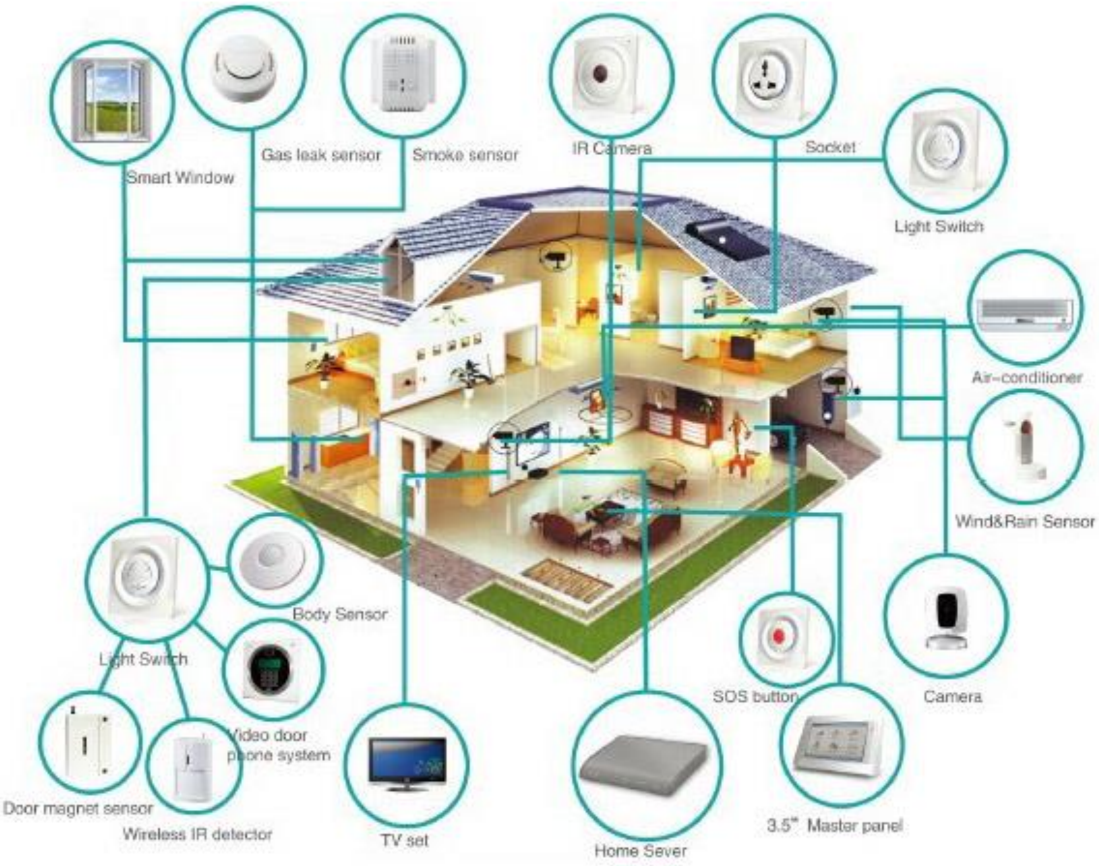


Figure 2.7 Smart home Gadgets/Devices

Source: https://three-s.co/solutions/smarthome-solutions/

Since the late 1970s, the concept of home automation has been around. A SM can be defined as a home or household that is created with mechanised systems in which the equipment are constantly communicating with one another. These automated systems allow the resident to monitor and control all of the household's units. Smart houses refer to an interior system that allows users to control equipment remotely and automatically via the internet using a device such as a smartphone. A really smart house is capable of not only connecting, but also "thinking" on its own. Smart homes can start making wiser judgments when data from numerous sources is collected, stored, and evaluated. **Gartner** defined connected home solutions as "Connected home solutions consist of a set of devices and services that are connected to each other and to the internet and can automatically respond to preset rules, be remotely accessed and managed by mobile apps or a browser, and send alerts or messages to the user's".

Smart Home, Connected Home, and The Smart Connected Home are the three subcategories of the overall Smart Home.

- **Smart home** - A SM is built on the idea that permits residents to use home appliances that are local to their home. This system is based on a wired-based standard that is not connected to the internet and focuses on light and window automation.
- **Connected home** - A Connected Home is distinct in that it lets remote control via the internet. Security and health management are common services provided by this sort of residence. Typically, the system is controlled by a gateway that may be accessed by a smartphone.
- **Smart connected home** - A Smart Connected Home is built on a system that combines the two types of smart homes discussed above, as well as the ability to learn. This type of house's system may learn a variety of factors, such as a resident's forecast and lifestyle within a home environment. Cloud services and tools for analysing data are frequently employed while building this form of Smart Home. These services can perform independent activities if they are

required by the system. If a water leak occurs and a smart leak detection system is installed, the system will alert the user that there is a place and most likely where the leak happened.

A Smart Home is now considered the same, though it is more advanced and can be utilised for a variety of purposes. As stated in (Surinder Kaur, 2016) the Smart Home is used for comfort, safety, and security, as well as to be more cost effective and allow residents to regulate their energy use, which is beneficial from both an economic and a comfort standpoint.

2.8.1. How does smart home function?

Home automation (HA) works using a network of devices that are connected to the Internet via different communication protocols, such as Thread, Wi-Fi, Bluetooth, Z-Wave etc. The devices can be managed at a distance via electronic media via controllers, either a voice assistant like Alexa Siri, or mobile application. Many of these IoT devices include sensors that detect deviations in motion, atmospheric pressure, and illumination, allowing the user to learn more around the device's surroundings. The user triggers actuators, which are physical process such as light buttons, electric controllers, or engines that allow gadgets to be managed remotely, to make behavioural change to the device. For setup and control, almost all devices require an app, which is often installed on a smartphone or tablet. The app is the primary way to interface with the device and establish things like schedules, as well as connect it to your preferred smart home ecosystem so you can setup Schedules and Automations for all of your smart devices.

Even the most technologically challenged person can readily set up and install these, while most gadgets require professional installation.

2.8.2. Best Smart home ecosystems

(source - https://www.sciencefocus.com/future-technology/smart-home-the-best-automation-devices)

- Apple HomeKit
- Amazon Alexa

- Google Home
- Samsung SmartThings

Apples Homekit - Apple's HomeKit platform is the most user-friendly and dependable smart home ecosystem available. Because all data connected to your house is handled locally and encrypted before being sent to the Cloud, it's also incredibly secure and a fantastic solution for individuals concerned about privacy and the smart home. It connects with all of your Apple devices, so you can use your iPhone, iPad, Mac computer, Apple Watch, and Siri to control your home. For wireless connection, HomeKit utilises Bluetooth, Wi-Fi, and, most recently, Thread. There are few limitations of this apple Homekit, very fewer HomeKit-compatible gadgets are there than other ecosystems, however the list is rapidly growing.

Amazon Alexa - The Alexa smart home system is centred on the company's unique AI speech assistant. It is the most comprehensive, interoperable, and affordable smart home ecosystem - Alexa works with more devices than any other. With the addition of a Zigbee radio to the popular Echo speaker's Wi-Fi and Bluetooth capabilities, it can now connect to even more devices, including as motion sensors and light bulbs. Alexa is embedded into a variety of smart speakers, smart screens, and even a smart thermostat and smart light switch, with prices starting at 5000 approx. In a nutshell, it's all over, making it incredibly simple to set up a reactive, voice-controlled Modern home. There are a many items that Work using Alexa. But not all of them work properly. It's a pretty open environment with little regulation, so do your homework before purchasing any device to ensure it functions the way you want it to. Alexa is difficult to use on a smartphone.

Google Home - Google Home is the name of Google's home ecosystem, as well as the app that you use to operate it from mobile phone. Google Assistant is the company's digital assistant, which is available for voice control of your devices. Google Assistant is now available as a mobile app on your Android phone or smart watch, making it simple to access its services no matter where you are. When you don't want to utilise speech, the Google clever displays – Nest Hub and Nest Hub Max – provide a touchscreen control panel for controlling lights, temperatures, locks, and speakers. Google is still far behind in terms of smart home gadget compatibility but getting up to speed up fast.

Samsung SmartThings - SmartThings is one of the first smart home hubs, and it supports the widest range of smart home devices, including nearly all Samsung electronics and appliances (TVs, washing machines, fridges). Along with Zigbee and Wi-Fi, it's also the only ecosystem in the area that can control Z-Wave devices. Z-Wave is a significantly lower-powered alternative to the other protocols, allowing for smaller devices due to the lack of large batteries. Z-Wave, like Zigbee, does not require communication with the Cloud and instead communicates with its hub, making it more stable and responsive. It is possible to combine the power of both ecosystems by connecting SmartThings and Alexa. Smarthings is a one of the greatest difficult system to use. However, this is also due to the fact that it is the most powerful system available, with the potential to perform more complex home automations.

2.8.3. Smart home: Earlier, Current and future prospects

Smart houses are a subset of ubiquitous computing that entails embedding intelligence into houses for the sake of convenience, healthcare, safety, privacy, and energy conservation. In 1975, the most widely used home computerization system was developed based on X10 protocol. (sharda katre 2017). There are 3 generations of smart home (li et. al. 2016)

- 1st generation - wireless technology
- 2nd generation - AI controlled appliances
- 3rd generation – Robots that can reacts with human commands

The underlying roots of centralization and automation of private activities can be discovered in the 1st electrically-wired private constructions at the end of the 19th century. Home appliances such as Freeze, Washing machines, Irons, Toasters, and cloth dryers were invented between 1901 and 1920. Along with this in 1950 home Television were invented. These two inventions has lead the foundation for remote control activities. Electronic computing Home operator (ECHO IV) and Kitchenette Computer are invented in 1966-1967. The ECHO IV was the first outstanding device. In the 1990s, the state of the art was the Internet, which created a holistic system of PCs. Remote Internet, often known as Wi-Fi, quickly became a common device in American households. The early 2000s saw a boom in clever home innovation, with service electronics, home systems administration, and a variety of new devices appearing. In the same era the Z-wave technology has starting connecting many of the devices like smart locks and flood monitoring technology.

IOT has empowered clever innovation to become a clear part of daily lives in past few years. Smart home technology can manage everything from fridge to thermostats to home security. Home devices are vital element of the IoT when they can be watched and organised remotely by the use of the Internet. Smart homes today are further concerned with security and living more sustainably. Remote flexible control, computerised fairy lights, automated indoor alteration, transferrable/email/content alerts, and remote video surveillance are all current trends in house mechanism. Sensory system serves as a home system's eyes and ears.

As we are progressing into the next generation, more and more appliances will start to communicate with each other. The goal is to create a world in which data is exchanged between machines and humans without the need for human interaction.

2.8.4. Home owners’ expectations from smart home

- **Security & safety** – The safety of home owner is really important. This applies to both indoor and outside settings where the residents are present. People are increasingly being forced to monitor their houses for outside intrusions or to check on the well-being of their children or elderly relatives who are staying at home.
- **Safeguard privacy** – While connectivity and automation are necessary, no one wants to jeopardise their privacy or safekeeping. Most smart devices being able to interconnect with one another locally or via the cloud, data outflow must be prevented wherever possible. Home users are concerned almost security risks and weaknesses that could compromise user’s personal information. The term "privacy" denotes to the protecting and safety of personal information.

- **Cost efficient** – The majority of clients are always price conscious. They require solutions that are cost-effective. If prices are cut, smart home adoption and adoption will increase.
- **Comfort** – Home owners always expects peace of mind and comfort from smart technology. Smart homes allow you to better control environmental parameters such as temperature and humidity, improving your quality of life.
- **Convenience** - With the advancement of technology, a client expects to be able to fix his problem in a short amount of time and with minimal human participation. A customer, in general, likes an automated environment that increases his quality of life.
- **Ease of use** - consumers expects ease of use in operation so that non-technical people can also use it efficiently.
- **Energy saving** – In most countries, energy is one of the most expensive commodities. As a result, customers are more conscious of their energy consumption. They must be able to manage and alter their energy usage and trends.
- **No-Hassle system** – The system should not be too difficult to use or perceive. The expectation of the home owner or user is a bug-free and threat-free system. Overall, automation is expected to result in increased comfort, more personalization of the environment, and fewer inconveniences.
- **Proactive technology** - In accordance with the preferences made, a client anticipates a greater quality of life, convenience, and smart automation. With virtual reality, a personalised home with an intelligent system that understands the occupants' needs and maybe moods is no longer a faraway fantasy. It has made advances all over the place.

2.9. Issues related to Smart home technology

The smart home industry faces many security problems, like any other technology may face. Both Hui, Sherratt, and Sánchez (2016) and Nixon, Wagealla, English, and Terzis (2004) stating that security risks arise with every technology, greater security precautions for smart home technologies are required. Smart home technology, in especially, is appealing because it allows a variety of devices to be linked together.

Smart home gadgets and services can be subject to a variety of security risks, and because the technology is used in one's house, the user's privacy, confidentiality, and reliability may be compromised. Since maximum of the devices and the communication between them are wireless, the technology is subject to assaults such as eavesdropping. In addition, the gadgets are left unattended, making them open to physical attack. These components' security mechanisms may be weak since they are frequently simplistic, with a limited user interface and limited processing capabilities. (Atzori, Iera & Morabito, 2010).

Kabalci (2016) has identified many security vulnerabilities associated with smart grid technologies, including the issue of thousands of linked devices. Smart grid security risks are classified as connection-based or device-based, with connection-based threats including eavesdropping and protocol breakdowns, and device-based threats include DoS attacks and Man-in-the-Middle attacks.

Stojkoska and Trivodaliev (2017) Also mentioned is how smart grids might be a target for cyber attackers, as well as how the major role of IoT devices is to link and transfer data between one another, making them subject to the most frequent assaults that might damage a wireless network. So author also propose that an IoT security strategy is required, but that the expenses be kept as low as possible.

A study made by Wilson, Hargreaves and Hauxwell-Baldwin (2017), According to the findings, when firms in the smart home manufacturers advertise, they do not place enough emphasis on data security and privacy, which causes potential users of the technology to lose faith in the goods. However, it has been proposed that the way a company advertises itself may not truly represent its current state. Their research looked at how potential users of smart home technology in the United Kingdom perceive advantages, hazards, general concerns, and design features.

The findings revealed that respondents believe that regulating energy, heating, and lighting are important.

The primary purpose of smart home expertise was to provide ease and security at home. When questioned about the possible hazards of smart home technology, the results revealed that reliance and losing control of the house were the most prominent worries. (Wilson, Hargreaves & Hauxwell-Baldwin, 2017).

The apps given by smart home technology businesses should also be able to offer privacy, confidentiality, and safe data storage for their consumers, according to the discussion. Companies that sell smart home technology should be able to demonstrate their reputation and have the necessary resources to provide performance guarantees. The lack of standardisation has also been investigated and explored. When it concerns to network routing for IoT devices and the reliability of that routing is important.

Airehrour, Gutierrez and Ray (2016) identified that either a new or upgraded security protocol or identification procedures for IoT devices are required. Batista, Melício, and Mendes (2017) in their study, which also was predicated on the idea of Industry 4.0, they focused on establishing a framework and structure for smart grid vendors. The authors observed a problem when smart houses and smart home technologies in several communities desire to connect and expand under the Industry 4.0 paradigm, therefore they created an architecture that would allow and support heterogeneous interconnection and growth. In their architecture, they also offered more security measures to mitigate potential risks and threats in the future.

They also included extra security features in its design to help reduce future risks and attacks.

2.10. Reason behind studying Security and privacy

Smart homes generates considerable quantity of data (big data) through sensors concerning health data, financial data, Personal conversation data related with safety etc. which is very much private and sensitive in nature(Joseph Bugeja 2016). The user have no control over the information sharing process. Due to the openness of internet system can be manipulated or attacked by intruder.

- **Massive private/sensitive data** - Smart homes have the ability to gather vast quantities of data (big data), some of which may be extremely sensitive, such as behavioural trends, medical data, living environment etc. When no one is looking, actually machines are watching you. But also details about your area, the location of the user. There are many examples that peoples home camera were compromised and displayed on the Net.
- In the smart home, the information circulation process is usually performed outside of the users' control. This is another example of how much is achieved without the user's knowledge or consent.
- Smart home systems, like everything else on the Internet, can be hacked, stolen, or targeted, affecting not only the personal but also the private, and not only the digital but also the offline lives of users. In essence, this is why I find this field so fascinating to study. Here's a situation in which digital threats don't just stay digital; they come to life.

2.11. Security & Privacy risks with smart home technology

- Toschi, Campos and Cugnasca (2017), in their research, they also found that the marketplace for communication standards is diverse, and that not all devices are compatible, and that only compatible equipment and goods may be utilised under the same communication protocol.
- Zigbee (2017e) According to them, out of so many communication protocols, theirs provides connection for the widest range of items. What Company A defines as ideal, a single public protocol that everyone uses, may be a dream come true for businesses, allowing everyone to utilise all of their products, however as describe (2017) and Zillner and Strobl (2015) stated, Other security threats associated with the products and protocols, such as implementation issues and improperly configured settings, are also mentioned.
- Gill et al. (2009) also discovered were flaws during deployment that might jeopardise the security of smart home technologies. Smart lights from Phillips that used the Zigbee protocol might be hacked, as a team of researchers from the Weizmann Institute revealed. (Charlton, 2016), Despite the fact that Zigbee later indicated that the hack was not due to Zigbee's protocol, but rather to a design software development flaw and fault, (Ricker, 2016).
- This event demonstrates how the various parties involved, including a corporation that delivers a product, a communication protocol, and the end customer (the one who implements the product), respond to a security compromise. The duty for the many people involved moves, and the same may be said for the firms examined, who have suggested that accountability may not always be with them it is hard to drawn conclusion.
- Cook and Das (2004) had stated in their research that a common communication network is what is hoped for, however it seems impossible to accomplish since there is too much diversity today in devices and products, and all these have different requirements. Where the responsibility for security would fall would be another problem which would have to be investigated.
- Jacobsson, Boldt and Carlsson (2016) has earlier indicated that the most essential period in which corporations and manufacturers must be aware of security risks is during the product design phase. As companies try to meet the

demand and interest for new and innovative technologies, it's critical that security is considered during product development, and as companies try to meet the demand and interest for new and innovative technologies, it's critical that security is considered during product development, and as companies try to meet the demand and interest for new and innovative technologies, conveyed, the design stage is of greatest significance.

- If organisations are attempting to fulfil demand and interest, there may be pressure to provide items as quickly as possible, which can lead to mistakes throughout the development phases and overall security concerns. Due to the fact that they were founded not long ago, the enterprises questioned in this study may be classified as small businesses.
- As Kshetri (2017) There are various obstacles that the smart technology sector must overcome, according to the findings. The issue voiced when it comes to the security of smart home technology might be attributed to two things. First, as both Hui, Sherratt, and Sánchez (2016) and Nixon et al. (2004) noted, China lags behind in software development. Smart home technology's security must be considered in the same way that any other technology's security must be considered. However, the concern is heightened because more devices are connected in a smart home solution, and the location in which they are implemented is in someone's home, which can be deemed more important and delicate.
- The second problem is that businesses may view their goods as simply that: goods, rather than computers with the same or similar vulnerabilities as other technology. In certain regions, there is a lack of quality, and there are currently few rules in place when it derives to privacy and security. One of the major challenges to attaining the goal of smart, energy-efficient houses and buildings has been identified as enforcing security in Internet of Things ecosystems. Understanding the hazards associated with the usage and possible abuse of information about houses, partners, and end-users, as well as developing techniques for incorporating security-enhancing measures into the design are all important in this context is not open and thus requires considerable examination. A risk analysis was carried out on a smart home automation system created as part of a research project comprising major industrial

players. The risks categorised as high were associated to the human issue or to the software issues. The findings show that by implementing conventional security measures, new and existing risks may be reduced to acceptable levels, however the most significant risks, such as those arising from the human factor, require more careful attention since they are intrinsically complex. The ramifications of the risk analysis results are discussed, and it is concluded that additional gene research is required. With such a paradigm of security and privacy in development in action, it will help to enforce system security and improve user privacy in smart homes, allowing these IoT settings to fulfil their full potential (Andreas Jacobssona 2016).

- The IoT is becoming more common in residential settings. Consumers are making their homes smarter by installing internet-connected sensors, lighting, appliances, and locks that can be controlled by voice or other user-defined automations. Concerns about IoT and smart homes have been noted by security experts, including privacy hazards and insecure and unreliable equipment. Nevertheless, the security and privacy issues of end users who build up and engage with today's smart homes have received little attention. To close this gap, we conducted semi-structured interviews with fifteen smart home inhabitants (twelve smart home admins and three additional residents) to learn about how they utilise their home automation and their security and privacy concerns, expectations, and mitigations. We discover gaps in threat models as a result of a lack of depth of understanding of smart homes, consciousness of some security issues but low concern, informal mitigation and an inconsistency between the concerns and strength of the smart home owner and other people in the home, among other findings. We make recommendations for smart home technology design based on these and other results. (Eric Zeng 2017).
- Smart Home innovations have the power to improve people's lives, boost home security, and make senior care easier. As a result, they need access to a lot of information on the users' homes and personal life. As a result, security and privacy issues are a significant roadblock to this promising technology's adoption. Dedicated to assisting end users in making well-informed decisions by addressing the constraints. Their many worries were grouped into four

themes: assaults on Smart Home systems and data, the projected sudden loss, the trade-off between utility and security, and user-centric issues and societal issues. Second, from an interdisciplinary standpoint, author examine measures to address the four issues. The article concludes with suggestions for resolving user concerns and assisting developers in the development of user-centric Smart Home technology (Verena Zimmermann, 2019).

- If surveillance applications in private contexts, such as smart homes, are to be approved by the residents, a privacy management strategy is required. Because of the intrusive nature of monitoring and the private character of the house, this is the case. We present a framework for dynamically modifying the privacy policy used to the tracking of a smart house platform in this study. Author first assess the scenario, or context, in the environment. We next identify many elements for detecting environmental context and present techniques for quantifying it using audio and binary sensor data. The context is then translated to a suitable privacy policy, which is accomplished by using data concealing methods to limit access to data obtained from multiple sources. The importance of this research is that it looks at privacy problems in assisted-living smart home situations. In such applications, a singular privacy policy will be either too restricted for a watcher, such as a caregiver, or too intrusive for the inhabitants. We address this by presenting a dynamic strategy with the goal of reducing the technology's invasiveness while retaining its effectiveness. (Simon Moncrieff, 2018).
- The integration of IoT devices into daily life poses privacy issues for its users and others who are impacted by these devices. This study investigates the variables that influence human concerns about IoT use, as well as how those variables influence the dynamics of privacy management when an IoT device is present (Ali Padyab,2018).
- As of their privacy-invading nature, user privacy has been a key consideration in the development of IoT services in recent years. However, there has been relatively little study done to date on consumers' perceptions of privacy in relation to IoT. Researcher want to know how and whether contextual variables influence users' privacy perceptions in IoT settings in this study. Researchers used a public online survey with 236 respondents and telephone

interviews of 41 respondents to investigate factors that can impact privacy perceptions. Despite the fact that several participants highlighted privacy threats in IoT and gave the acquired data items a low rating, we discovered that a large number of participants would still choose to use the offered IoT service if they find it useful and practical for their daily lives, despite the potential for privacy infringement. Finally, we analyse and emphasise the qualitative feedback. (Ismini Psychoula, 2018).

- A smart grid is intended to enable a more profitable, eco-friendly friendly, supportable and reliable supply of electric power. However, important security problems for the smart grid must be addressed; risks vary from a threat to energy supply to a threat to consumer privacy. This article outlines a strategy for identifying security risks in the smart home environment, as well as assessing their severity and importance. The approach can also reveal new hazards that haven't been explored in the literature. The smart home situation is signified by a context-pattern, which is a specific kind of pattern for the induction of domain knowledge (Airehrour, 2016). As a result, by substituting a context-pattern for another domain, such as clouds, the approach may be used to these other domains as well. The concept is based on Microsoft's Security Development Lifecycle (SDL) (Atzori,2010), which employs Data Flow diagrams for scenario definition and asset identification, but presents novel context-pattern-based options for scenario definition and asset identification. These help to relieve the problem. Kristian Becker, 2008).

- As the world moves toward the Internet of Things, smart homes are swiftly becoming a reality. Home appliances and equipment are connected using proprietary or standard TCP/IP protocols to form a home area network, allowing for improved administration and monitoring. Smart homes, like any other network, are vulnerable to security threats and vulnerabilities. The purpose of this study is to demonstrate the significance of security in the context of smart homes. We will discuss (a) the definitions of a smart home system, (b) various home automation communication systems, (c) security issues and problems in a smart home, (d) security risks in a smart home system, (e) existing security measures to combat such attacks, and finally, supposition and future work (Shafiq Ul Rehman ,2016).

- Smartphones have exploded in popularity since the year 2000, making people's life easier. New smart products, such as tablet PCs, smart TVs, smart refrigerators, and smart air conditioners, have appeared since the introduction of smartphones, broadening their applications from individuals to businesses and homes. As a human-centric business, smart home service has gotten a lot of attention lately. This is the environment in which home appliances and other smart gadgets are connected to the internet for the purpose of providing better service and experience to users. To perform the function of linked home, the existing smart home service relies solely on a wireless home network. Because the service lacks smart home security, consumers may incur financial losses as a result of data leakage or home appliance malfunction. The security of smart gadgets must be taken into consideration. We offer an improved security architecture for smart devices in a smart home setting in this research. For combating security risks such as data alteration, leakage, and code fabrication, the security framework includes an integrity system that uses self-signing and access control approaches. (Won Min Kang, 2017).
- The proliferation of IoT devices in various areas of our daily environment has come from the introduction of IoT technology, which provides many benefits to our lives. However, in order to keep up with the fast changes in the IoT industry, many IoT devices were extensively deployed without security by design being implemented at the time of development. As a result, hostile attackers have turned their attention to IoT devices, particularly those that lack security features. An attacker could take control of home IoT device with insufficient security protections, such as the Mirai Botnet. By launching a DDoS assault on a DNS service provider, the IoT device may bring down many websites. As a result, in order to improve the security of the IoT service environment, this study suggests a strategy to reduce security vulnerabilities and risks in IoT devices. (Seul-Ki Choi, 2018)

Privacy risks

With the rise in popularity of smart homes, various security concerns have arisen regarding scalability and interoperability issues among IoT devices. In terms of assault frequency and complexity, threats are increasing at an exponential rate. However, networked home devices are exposing more than just security vulnerabilities; they are also raising severe privacy problems. Because of the nature of smart homes, users are exposed to a variety of privacy risks, such as an unauthorised party gaining unwanted or improper access to their personal information, to psychological characteristics of privacy (aloneness, separation, privacy, intimacy), or even a physical violation of privacy in which an unauthorised party gains entrance to the home itself is accessed by unauthorised party (Fraser Hall and Leandros Maglaras, 2020).

- **Storage by a third party on cloud**

  The emergence of third-party cloud storage played a significant role in the development of the smart home function that allows remote access and monitoring [14]. This allows you to access data from your smart home from anywhere. A third party could store an alarming amount of personal data and private information. It was also the situation with Orvibo, a Chinese firm that operates an IoT service offering. They were the victims of a data breach that resulted in the exposure of 2 billion records related to smart home devices. Passwords, account reset codes, precise geographical location, and scheduling information was exposed to the hackers. Smart home can provide attackers with knowledge about user routines and whereabouts, potentially permitting theft opportunities by determining when houses are empty. Because attackers now have access to some of the devices, such as smart door locks or surveillance cameras, the knowledge might render them unusable.

- **Secondary use of Data**

  Users can ask questions and interact with the device by speaking to it. Workers analyse voice samples provided to the device in order to improve Amazon's speech recognition software.

  This raises certain worries about data that may be gathered accidently by the gadget. Users' private talks in their homes may no longer be so private. When analysing speech samples, two workers reported hearing what they think to be a sexual assault; this usage of data could lead to difficulties with confidentiality and morality.

- **Vulnerable to attacks**

  The proliferation of smart homes, as well as the variety and volume of IoT devices connected to them, has increased the attack surface area for malicious actors. Smart houses, according to Cyber Security Trends 2020, would be popular targets for bad actors due to the large number of potential access points. An attacker who gains access to a single smart gadget in the home has the ability to cause havoc. The personal information and private data (eavesdropping attack). In 2017, a German government authority ordered parents to trash a talking doll named Cayla. The inbuilt Bluetooth device was revealed to be vulnerable and could be abused, allowing an attacker to listen in on and talk to the youngster who was playing with it.

2.12. What is big data?

Big data refers to the data that characterizes the 4V’s - volume, variety, velocity and veracity. It refers to collections that are too large for traditional database applications to capture, store, handle, and analyse. Large organisations, such as health care, banks etc experiences lots of difficulties in keeping all of their data coming from alternate channels on one platform at a single, reliable site. This one-of-a-kind task of making analysis of the information coming in from various sources and extracting valuable actionable intelligence is what we now refer to as Big Data. The magnitude of the data sets often referred to as data volume that needs to be examined and handled are much larger than terabytes and petabytes. Variety of data means data structure. It can be classified as structured, unstructured, or semi-structured. Care-related activities have unstructured data, while financial and some medical data can be more structured (V. Vimarlund, 2014). Data velocity is linked to its speed of generation- constant or real-time, for example traffic data. Big data, on the other hand, necessitates sophisticated techniques and technology in order to collect, store, distribute, process, and analyse reliable data. As stated by Geethumohan (2019), the combination of two evolving technologies IoT and big data can be utilised for better managing energy utilisation in homes as well as in industry.

2.12.1. Big data analytics techniques

Apache foundation developed open source components make up the Hadoop ecosystem. This gives a framework for big data management. Meaningful insight and predictive analytics is offered by data analytics tools which is a part of big data framework.

Following are the components of Hadoop framework along with big data analytics tools (Youssef Gahi, 2016).

- **HADOOP** - The Hadoop diagnostic tool is an open source programme designed to analyse large amounts of data referred to big data. It is a non-relational database system that manages a large volume of dispersed dissimilar data. It's an excellent foundation for other applications that seeks to do parallel computations on big amounts of data. Hadoop has two primary functions: storing and calculating. Hadoop divides the data into partitions.

- **MapReduce** - is a Google tool for processing enormous amounts of data. It has two different working modes: Map and Reduce. The input data is sent to various clusters for parallel processing in the first part. The Reduce section entails gathering all sub-results in order to deliver a single final report.
- **HDFS** - Hadoop's core is the Hadoop Distributed File System. It's a dispersed file system for data warehouse storing and management. HDFS can hold petabyte-sized data across numerous nodes or clusters. It accomplishes this by dividing the incoming data into chunks and then allocating these blocks to servers in various places.
- **Hive** – Hive is data warehouse that permits you to access and manage large amounts of distributed data. Hive gives you the ability to connect to the internet storage with the use of a SQL-similar language called HiveQL is a query language for the hive.
- **Cassandra** - Cassandra is a columnar NoSQL database built by Facebook. Casandra give backings MapReduce handling and is well-recognised for making data access for a vast number of data samples.
- **HBase** - The Hadoop DataBase is called as HBase. It is a disseminated database managing system based on BigTable from Google. It is a strong database for managing and analysing large tables with heaps of columns.
- **PIG** – PIG is a programme development platform for MapReduce. PIG Latin is the name of the programming language, purposes to improve Hadoop and MapReduce speed by providing a software programming tool that allows for rapid processing.
- **NOSQL** - Not Only SQL encompasses all non-relational databases. It allows you to search for and retrieve unstructured and semi-structured data.

2.12.2. Big data IoT & Smart home

The Internet of Things (IoT) and Big Data analytics have melodramatically changed the computing industry's landscape. We have all witnessed fantastic changes in our daily routines as a result of technical advancements, and even these things have witnessed tremendous insurgencies that were not even considered technologically handled. I'm specifically referring about smart home technological advancements. Big Data is said to have had a tremendous impact on numerous areas of the economy in recent years. Specific software is utilised to indicate trends and patterns in human behaviour for this aim (Ejaz Ahmed, 2017). The technology has had a significant impact on how we run our houses. Any home may converted a smart house by the support of technology. As a result, many IT professionals are focusing on Big Data analytics for smart homes. Presently new gadgets with safety sensors have appeared. All of these devices are controlled by our smartphones and tablets and are connected to the Internet. The IoT is a term used to describe this viewpoint. The primary tenet of this concept is to run fully on automation. Home automation technology allows all gadgets to be controlled remotely once an IoT system is engaged. Because they can understand and analyse user data, these linked gadgets are intelligent. Security firms can use this information to gradually strengthen security measures. Furthermore, this data collecting aids in the improvement of consumer comfort and safety. Heavy data is mostly utilised to enhance consumer psychology in a typical corporate scenario. Opinion leaders frequently employ this technique in order to make well-informed judgments based on data analysis. Another important argument is that security firms are better equipped to uncover and correct flaws this way. Companies are responsible for increased fiduciary risk when they update their security systems. There is also a benefit for the consumer. The reason for this is that you may use this information to create virtual security barriers at home to keep attackers out. You can effortlessly monitor your home using smart home devices. As a result, you will be able to manage your intake and make the required lifestyle modifications. Traditional security technologies lacked the ability to sense and guard against fraud, attacks, and other threats. Over smart cyber hackers can readily breach an organization's operations to obtain confidential data such as intelligent property, credit card numbers, and customer databases in order to harm the company. Anomaly and fraud detection based on big data analytics may be possible (Aditya Dev Mishra, 2016).

2.12.3. Application of Big Data in Smart Home

Smart houses with advanced automated systems, such as light control systems that save energy, full or semi-automatic gate openers, motion sensors, IP enabled cameras, security alarms and safety notification systems, and door locks with thumb impression, give enhanced safety and security. This type of automated system in smart homes will necessitate an innovative technology that will provide an unbroken and consistent internet connection amongst the transmission devices and sensors of various home appliances, allowing them to store, process, and analyse their data. This can be accomplished efficiently through the use of the IOT and related technology in smart homes (Abhay Ray,2016).

A smart home can create various types of data and employ various mechanised and technological organisms. All devices produce and store data in the similar file layout or employ the equal access technique. The most common types of data produced by a smart home are listed below.

- Streams of footage from IP-enabled CCTV cameras
- Security and management of entrance gates of smart home.
- Logs of entrance gates entry and exits
- Data for electricity use, availability and backup
- Data for home appliances such as intelligent lighting, heating system, smoke detectors and robotic vacuum cleaner
- Data regarding home cleaning and sanitisation
- Information of security alarms and safety notification

Over all, smart homes are a big source of data, and it is estimated that a smart home can generate at least 1GB of data per week. So, if we examine the data generated over a period of five years we have a huge amount of data that is unlikely to be managed using a traditional database system. As a result, these types of systems (smart homes) should embrace big data technology and tools. The most significant benefits and major advantages of using big data is- tools like Hadoop and its companion tools enable large scale data processing (Map reduction operations) at a low cost, regardless of the data's structure. Big data's tools are usually open source, and offering cloud-based analytics facilities. This makes them less expensive than previous technology.

Through analytics scripts and tools, smart homes are constantly demanding both faster and better decisions for all application, including safety, reliability, security, access restrictions, visual reporting with appropriate alerts / notifications. Many enterprises, smart cities and smart homes are concentrating on speeding up their decision making. This is because of the inbuilt features of Hadoop like fast processing capability, security features, data replication function and in-memory analytics.

By using advanced analytics, a smart house user can monitor his data from any remote place via a secure connection in his required format. In the later stages, the service provider agencies can easily integrate and develop applications for the smart home owner on his request. Keeping the benefits of Big Data in mind, Vendors can leverage Big Data in the installation & configuration of smart home technology to keep things running smoothly.

2.12.4. Big data analytics for security challenges –

Recently Big Data are used to improve information security. The most common reason for using big data analytics tools is to evaluate and store trends in the datasets gathered for business purposes. Anomalies or fraud are identified using big data analytics in several domains such as insurance, medical services, credit cards, internet banking, so on and so forth. Big Data analytics can be used to discover fraud and suspicious activity by analysing network traffic, financial transactions, and log files, as well as combining different sources of data into a logical view. Sophisticated big data innovation, like Hadoop related databases and streaming analytics, is supporting the collection and analysis of massive amounts of mixed data at an extraordinary scale and speed.

Security analytics will revolutionize these types of systems by collecting data from various sources such as vulnerable data centres, will then perform comprehensive analytics on the collected data, and finally accomplish real time analysis of data to build up views on security associated information.

It is important to highlight that in order to correctly characterise the "Big Data analysis tools," analysts and system architects still need information about their systems.

2.13. Smart home gadgets and technology: Vulnerabilities

Understanding the risks of an individual IoT device and their consequences will help consumers appreciate the importance of taking a strong security stance when planning for smart homes. This entails examining the wide variety of smart home systems that could be compromised. These devices can operate against users' comfort and instead become instruments for compromise and chaos (Jiv chang 2019).

Following are the serious threats created by connected devices.

SN	Gadget	Functions	Technology/ Sensors	Vulnerabilities / Threats
1	Smart wireless Speakers	You can talk to it & control the things by voice command. The apps offer access to music system and other streaming facilities to offer great resilience	Speech recognition Wireless communication continuously listening microphones Bluetooth Microphone	• Insecure access control • If hackers can take unauthorized control, they can play with devices in home and create chaos.
2	Smart Security Camera	Allows for high-density video recording and adjustment to changing light levels across the day. Software such as broad Dynamic Range, that balances the sunlight in a video after it's been captured, and video compression, which allows users to save more data, are also available.	Image processing Cloud computing	If hackers can take unauthorized control, They can record and take away unwanted recordings (threat to privacy), potentially steal private information (threat to security).
3	Smart Air-conditioner	Smart air-conditioner allow user to remotely control home's temperature through Smart phones or internet-connected devices. It provides energy saving features along with continence. These gadgets also	Wireless communications Machine Learning	If hackers can take unauthorized control, Can disrupt the Air conditioning system (making the house environment uncomfortable). Also, this may lead to increase electrical consumption (increase

SN	Gadget	Functions	Technology/ Sensors	Vulnerabilities / Threats
		learn from homeowners' habits and adjust settings automatically to deliver optimal comfort and efficiency to inhabitants.		in the bill)
4	Smoke Detector	Smoke dictator is a fire-protection gadget that detects and warns of the existence of smoke autonomously.		If hackers can take unauthorized control, • It can create malfunction – unwanted turning on the water sprinkler system (which is wastage of water and damage to system) • When needed, it may not turn ON the prevention system (not turning the sprinkler system, not giving fire alarm). This can cause damage to assets
5	Smart locks	Lock and unlock doors with the tap of a finger. Basically allows keyless entry to home	Access control Wireless communications	If a Home Monitoring system (which includes smart locks and motion sensors) is hacked, an intruder can gain access to the property without using force. (A hacker who gained access to a smart home's security vulnerabilities discovered that he could not only unlock the door lock but also jam the motion sensor.) Plus, there was no sign of it in the system at all.)
6	Smart TV	Smart TVs may be wirelessly linked to a variety of input devices to improve usability and control.	Ability to connect to other wireless devices like smartphones	Smart TVs have cameras and microphones integrated in to help with face and speech recognition.

SN	Gadget	Functions	Technology/ Sensors	Vulnerabilities / Threats
		Text entry, navigation, and Web surfing may all be facilitated by connecting wireless keyboards and mouse, cell phones, and tablet PCs.	Voice recognition	Once a smart TV has been hacked, it run the risk of it recording films and audios without your knowledge or authorization. These audios or films might subsequently be used to steal your identity or blackmail user or family members by being posted on unsuitable websites.
7	Smart Refrigerator	Internal cameras, more adjustable user-controlled chilling choices, and the ability to interact with its functions via your smartphone or tablet while away from home are all elements of smart refrigerators. It will enable you to keep track of all perishable foods. The refrigerator's energy usage is also given along with these information. Food Manager and Grocery are two of the applications available.	Wireless communications	Cyber fraudsters can gain access to your online grocery store's login information and place undesired orders on your behalf if it is compromised.
8	Robot vacuum cleaner	Without the need for human involvement, a robotic vacuum cleaner mops floors automatically. This amazing vacuum cleaner glides around the table legs and corners of the room it's sweeping. When you are not at home, you may clean your	Wireless communications	If hacked • Unnecessary more cleaning (increasing electricity bill) • Potential damage of other equipment

SN	Gadget	Functions	Technology/ Sensors	Vulnerabilities / Threats
		house.		
9	Water leak detector	Closes off the water supply after detecting a leak and also sends alerts on mobile. Keep your home safe and free from extensive damage.	Wireless communications	If hackers can take unauthorized control, • It can create malfunction – unwanted alarm • When needed, it may not turn ON the prevention system. This can cause damage to assets
10	Wireless Smart lighting controlled through mobile app	Smart lighting is a type of lighting that is meant to save energy. Improved performance and automated tools that adapt based on factors like as occupancy or daylight availability are examples of this. The purposeful use of light to accomplish some attractive or practical effect is known as lighting.	Light sensors Wireless communications	An attacker can operate user policies, Status & messages and change the behaviour of Smart Machines at his want.
11	Wireless Door/Window opening sensors	It is an real security system that gives warnings you to any unpleasant activity noticed	Wireless communications	Hackers may remotely control windows and doors. Robbers could enter home when the property is empty.
12	Smart body analyser	This device measures both weight and fat mass and uploads the data to the hospitals' database over Wi-Fi.	Wireless communications	Data & Identity Theft Wearable's makes location based tracking easy
13	Garage door opener	Garage door is open or closed from anywhere in the world using smartphone app.	Wireless communications	
14	Wearable	Electronic technology or equipment placed into products that may be easily worn on the	motion sensors, temperature, proximity , biochemical	• protection of personal information from unauthorized

SN	Gadget	Functions	Technology/ Sensors	Vulnerabilities / Threats
		body are referred to be wearable. These wearable gadgets can monitor data in real time. They offer programmes that capture a picture of your daily activities and synchronize them with mobile phones or laptop computers. These gadgets can track things like the amount of steps taken, stress levels, sleeping habits, body wetness, and heart rate in the patient's environs.	sensors, Near field communication	access, use, or disclosure • Data may be shared or sold to third parties? • Hackers can easily hack the sensitive information by bruit-force attack

Table 2.1 Table Demonstrating Gadgets-functions-Technology-Vulnerabilities

2.14. Research Gap

After carrying out rigorous literature review, it was found that most of the literatures available on smart homes are limited to a very segment of systems i.e. energy efficiency, cyber attacks, network security, communication security etc. There are limited resources available that covers the complete implementation of the smart homes or to the remote server.

There is no specific study done on use of generic tools for data analytics on smart home application, though this area is beyond the scope of this research work. Application specific (like medical care or energy) have their own systems. This study tries to cover up this gap by conducting a complete privacy and security risk assessment to the entire smart home ecosystem. As many People have started opting for smart home technology, it is important to have a holistic system view of this paradigm (than being opportunistic approach). The User also needs to be educated on transparency of information, proper use of the system, adherence to the local rules & regulation.

The following gaps have been identified in making smart homes safe and secure

- **Network security**
  a. Hackers continue to take advantage of vulnerabilities in smart home devices. Their goal is to harm the smart home owners. This is because of the open internet connection.
  b. Many scams still rely on the poor security habits of a common man. However, if the protections of the smart devices are not improved, users' data becomes vulnerable for cyber attacks.
  c. Attackers are attempting cyber attacks that gives them opportunity to make easy money. Ransomware attacks have higher returns relative to other data stealing approaches.
- **Better understanding of privacy**
  a. The concept of privacy is not clearly understood by a common man. Unnecessary importance is given to that information which is easily available on public domain, for instance mobile number. This makes them feel that all data is private and needs to be secured. A correct understanding of privacy will also reduce the volume of data to be protected

- **Training awareness**

    a. Awareness is recognised as an important component in the strategy to counter threats. It has been found that there is an absence of knowledge on security among people across different age groups. There is no easy guideline available for a common man or non technical users.

    b. Those available are in product specific language that makes it difficult for a common man to understand. Hence users normally don’t follow these do’s and don’ts of security procedures.

2.15. Research Problem statement

During recent times, growth in Indian smart home users has increased many folds. Research conducted on Indian smart home users' shows revenue of US$ 4535 for the year 2021 which is predicted to reach US$ 6085 by 2022.

This indicates large Indian population have started or are intending to use internet enabled smart home device.

A smart home environment comprises of a digital mesh of interconnected device that communicates data related to different aspects of smart home application areas. Few examples include home security, surveillance CCTV's, video door phones, smart locks, smart energy metering, intelligent lighting, air-conditioning, so on and so forth. These devices collects massive amount of personal data which aggregates to significant amount of personal information.

Data generated by different devices in the smart home ecosystem characterize the features of big data and therefore big data analytics needs to be applied on these data to provide sustainable services to smart home users.

Certain data generated by the smart home ecosystem needs confidentiality. Data related to smart home users/ home member's personal preferences, passwords, security pins, health records for instance needs proper safeguarding.

But, large population of smart home users are not aware about following aspects of data:

- What kinds of data are collected from the devices which are connected in the smart home ecosystem?
- What kind of data can be collected from the devices which are connected in the smart home ecosystem?
- Which of these data are confidential and requires proper protection?
- What are the various ways to protect this data and in fact entire smart home environment?

Underlying idea is to protect the confidential data/information from falling into the hands of wrong people.

This research work will address the privacy and security issues in a smart home environment at various levels of its implementation.

This research will also provide recommendation to smart home users on following aspects:

- Selection of appropriate devices
- Configuration of selected devices.
- Networking and connectivity of smart home devices.
- Configuration of users using smart home system.
- Aspects related to data sharing with government agencies so that respective authorities can come up with new / enhanced legal framework to protect private information is also covered.

2.16. Research aims and objectives

This research aims at carrying out an empirical analysis on dynamic privacy and security assessment of the smart home environment using big data analytics.

To carry out this research work author has considered a sustainable smart home ecosystem that utilizes big data. Such smart home system do makes use of big data analytics in order to provide users an experience of pervasiveness. But, author has not carried out any work involving use of big data, big data analytics or related technology anywhere in this research.

Therefore, this research aims at the assessment of privacy and security of smart home environments which uses big data analytics.

The overall objective of this research is:

1. To identify the dimensions of privacy and security pertinent to smart home environment.
2. To study the impact of significant factors on smart home privacy and security.
3. To perform critical assessment of security vulnerabilities inside and outside the smart home environment.
4. To develop a dynamic conceptual framework of smart home ecosystem to mitigate privacy and security related threats/risks issues in smart homes.
5. To provide recommendations for the betterment of privacy and security of smart home users data (big data).

CHAPTER 3

RESEARCH METHODLOGY

3.1. Introduction

Research is a systematic investigation and review of materials and resources in order to create evidence and reach new conclusions. It is a careful consideration of the analysis of a specific issue or problem using scientific methods. Research is an original addition to the information that already exists. It means finding solutions to a particular problem in a systematic way. It involves in-depth research of the subject, observation, comparison and experimentation.

According to the American sociologist Earl Robert Babbie, "Research is a systematic inquiry to describe, explain, predict, and control the observed phenomenon. Research involves inductive and deductive methods."

Research methodology is the particular methods or techniques used to define, find, process and evaluate information about the topic. In a research paper, the methodology section helps the reader to objectively determine the general validity and reliability of the analysis. The Methodology section addresses two key questions: how were the data collected and how it has been analysed?

In common words, we claim that the primary goal of research is to find out the truth that is unknown and has not yet been exposed.

3.2. Rationale of the study

According to the literary survey, smart home technology is a relatively modern technology and it is growing at a rapid pace. This technology does provide the users lots of advantages like ease of operations, convenience, comfort, security and safety. If not used properly it can pose threat to the personal information as well as misuse of the devices used in the smart home ecosystem. The aim of this research is to study user's requirements about security and privacy related to smart home environment.

The real estate market in India is constantly growing and real estate developers are offering various facilities related to smart home like smart access entry, CCTV surveillance etc. There is an immense need to provide safe home which will protect the privacy and security of smart home user.

The findings from this study can benefit those home owners who would like to enhance their home security, privacy, reliability practices and better protection of their data. Improved data security practices may contribute to social change by reducing risk in security and privacy vulnerabilities while also contributes to new knowledge and insights that may lead to new practices.

3.3. Research objectives

Research objectives provide a detailed description of what the research is attempting to accomplish. They outline the outcomes that the researcher wants to meet. The research objective provides guidance for the thesis.

Research objectives of this research are:

1. To identify the dimensions of privacy and security pertinent to smart home environment.
2. To study the impact of significant factors on smart home privacy and security.
3. To perform critical assessment of security vulnerabilities inside and outside the smart home environment.
4. To develop an optimal and dynamic conceptual framework of smart home ecosystem to mitigate privacy and security related threats/risks issues in smart homes.
5. To provide recommendations for the betterment of privacy and security of smart home users data (big data).

3.4. Research questions

In this research work the questionnaire will address following aspects of a smart home environment:

- Which are the IoT devices most commonly used by smart home users?
- Are smart home users aware of the private information they share while using IoT devices?
- What are users’ perceptions on general security?
- Are users willing to share private data/information?
- Do smart home users have any knowledge about the data storage and devices safety?
- Do users have any idea related to the risks of using IoT devices?

- What are the recommended practices to follow in order to ensure protection of privacy and security in smart home environment?

3.5. Research Methodology

The research methodology used in this research work consists of- primary data based questionnaire survey. After rigorous literature review the factors important for assessing the privacy and security of smart home users are identified. A pilot research was conducted with a limited sample size and relevant factors are taken up in a final questionnaire survey. The questionnaire survey was conducted and responses were collected from smart home users residing in the state of Maharashtra. This research also contains experimentation based proposed framework Safe@SmartHome. The proposed framework is validated using case based method and is discussed in detail under data analysis chapter.

The sampling method used in survey is snowball sampling. As the smart home concept is relatively new in Indian context and is gaining popularity day by day domain, it was difficult to reach the users who were using the smart home devices.

Snowball sampling method often referred to as chain-referral sampling is best suited for this kind of research work; characterized as a non-probability sampling technique in which samples have features that are uncommon to find. This is a sampling technique in which current respondents provide data source needed for a research study.

Primary and secondary data are obligatory and essential for the analysis in order to study objectives and the achievement of the objectives. Primary data are collected through questionnaire survey and conducting formal meetings with respondents comprising working professionals, students and housewives from the Pune and other cities in Maharashtra.

3.6. Type of research

This research is an exploratory by nature prior to figuring out WHAT the problem is? It's experimental, in that we have found a solution to the problem. As a result, the analysis is covered in all aspects of smart home privacy and security. As a result, the analysis approach is a mix of qualitative and quantitative. The research is quantitative as it involves data survey and is qualitative as it involves study of user's perception towards smart home privacy & security.

3.7. Scope of the research

The scope of this research is limited to assessing the privacy and security of smart home environment using big data analytics. Every smart home ecosystem has three major components- the wireless sensor network, aggregation of big data and applying big data analytics on collected data. Author has picked up an area of data privacy and security, which in fact is related to data aggregation, and is considered one among the most important aspects in a smart home ecosystem. Big data and analytics related tools and techniques are not used anywhere in this research. The same is kept outside the purview. In smart home ecosystem various smart home devices generate big data and the service provider apply data analytics on this data to provide smart home related services to the users. Use of the term ”Bigdata analytics” is due to the reason that those smart home ecosystem are considered in this research that involves Big data and analytics.

This research aims to touch upon following aspects of smart home privacy and security

- Understanding users awareness on smart home privacy and security in reference to:
  - Smart home user's awareness on those data that which are collected by the aggregator in smart home environment. It further aims to explore user's understanding about the categorization of this data into sensitive and general.
  - Smart home user's concerns about security of the sensitive data/ information

Author has adopted following methods to achieve this purpose

- Literature review, in order to collect the details of research work carried out in the same or related area globally. This has also helped to understand the trends and evolving technologies for better user security.
- Formulating a research questionnaire to gather the information directly from smart home users. This was based on guideline presented under

section 3.4. Detailed questionnaire survey sheet is attached in annexure to this report.

    - Interviews with smart home solutions service providers / dealers, to understand prevailing technologies and user demand. This was done in a limited manner due to the COVID-19 pandemic situation, which has badly impacted face-to-face conversations

- To define the framework for better home security
    - Author has presented a frame work Safe@Smarthome. This will allow to understand:
        - Role based access control & strong encryption mechanism for improved security in smart home environment.
        - Methods of online monitoring for timely alerts and related action plan for damage control of smart home systems
        - Smart home system recovery plan (based on regular audits of devices.
        - Guidelines and documentations for selection of the devices and networking equipment along with best practices for appropriate configuration of the same.
        - Suggestions to improve the better access rules, improvements in system infrastructure, improved guidelines and updated user awareness training programs.
    - The framework will provide guidelines to all related players viz. actual home users, service providers, equipment manufacturers and government authorities in achieving solution for secured home environment.

3.8. Time for the research – As indicated in table 3.1, the study was done within the time frame allotted for it.

Activity	Duration
Literature review	12 Months
Identifying the factors relevant for research	3 Months
Rough draft of survey questionnaire	3 Months
Data collection for pilot survey	6 Months
Pilot study and dropping irrelevant factors	2 Months
Refining the survey questionnaire	1 Months

Data analysis	4 Months
Conclusion and interpretation from findings	3 Months
Preparation of final draft for thesis chapters	6 Months

Table 3.1 Time line of the study

3.9. Research Population & sample

Population - The total group of individuals, activities, or objects that the researchers want to consider is referred to as a population or target population. Individuals in the population have certain features in common. The target audience for this study is both smart home device users and smart home owners in the Indian state of Maharashtra. It would have been impractical to conduct this study on the entire target population therefore author has narrowed down the population.

Sample - A sample is a portion of a larger population. The sample is a designated group of certain elements drawn from the entire population. Anything can be learned and said about the entire population from the analysis of the sample. When a population is too large to perform surveys on all, sampling is used. The aim of sampling is to measure an estimated population feature. Respondents who knows the concept of Internet-of-things (IoT) and who were using smart home devices for more than six months and less than two years were preferred. Survey questionnaires were circulated among smart home owners and responses were collected. Google forms based survey questionnaire was sent electronically through emails and Whatsapp to smart home device buyers and smart home users for collecting the responses. Survey questionnaire were also collected manually through interviews.

Majority of responses were collected from Pune and adjoining area. Pune being an IT hub has representation of citizens from most of the regions across the India. In this regards Pune represents mini India. Pune's search for better urban living received a boost when it was named one of India's top 100 cities by the Union Government of India. As a result, the consumers have affinity towards small facilities in home. The result of this research could be an important reference for the smart home service providers, Builders, IoT product manufacturers, smart home IT/ITES companies in planning their business strategies and marketing.

The purpose of this research work is to understand the privacy and security related issues of smart home users and provide recommendation on the same. The research target audience are mostly residents from Pune city who have are either potential smart home buyers or smart home owners. The population consisted of smart home owners, students and housewives who are using smart devices in their homes. The concept of smart home is continuously evolving and their users are also increasing. Due to easy availability of technology information, through Google, social media platforms (like Facebook, Instagram) and other similar mean, people are now adopting the use of these devices at home. The cost of some of these devices is reducing and is becoming affordable. Considering the above it is practically impossible to define the population of available customers as and so it same as considering it infinite.

3.10. Sampling Frame & Sampling Methods

A sampling frame is a list or databank of potential participants from which a sample can be used in survey (Briony Oates, 2006). Sample frame can be used in qualitative and quantitate research. Sample frame mostly includes participants name, telephone number and emails id, so that they can be called to take part in the investigation.

Sampling is a method of choosing distinct participants or a subcategory of the population to create statistical interpretations from them and evaluate features of the whole population. It is practically impossible to study entire population for questionnaire survey. Sampling is a technique that lets researchers gather facts/data about a population founded on outcomes from a subset of the population, without investigating each person. The main advantage of this is, it reduces the time, efforts to obtain the good quality of information. Probability sampling and Non-probability sampling are two recognised methods of sampling.

Probability sampling is a sampling method in which a researcher selects a few standards and picks members of a population at random. With this selection parameter, all members have an equal chance of being included in the survey.

Non-probability sampling is a sampling method where researcher selects participants for study at random in non-probability sampling. This sampling method is not a predetermined or fixed selection procedure. As a result, it is impossible for all elements of a population to have equal chances of being included in a study.

Probabilistic	Non - Probabilistic
Simple random sampling	Purposive
Stratified sampling	Self-selection
Systematic sampling	Convenience sampling
Cluster / area sampling	Snowball sampling

Table 3.2 Sampling methods

Snowball sampling (chain or referral) - Snowball sampling is when participants are asked to refer other people they know who may be interested in participating in the study (for example, family or friends). When a researcher is unsure how to approach a specific group, they use this method.

In this research author has deployed snowball sampling method of data collection. In this data collection process few respondents were first approached then with the reference of these respondents further respondents were apprehended. This technique was employed as the population with specific characteristics is very less.

3.11. Sample size calculation

Formula for obtaining sample size

a. If mean (x) is applicable
b. S.D( ) is unknown
Considering the study none of the above terms applicable
For calculating the Sample size formula given by Prof. Yamne (1967)

$$Sample\ size(n) = \frac{N}{1 + (N\ ex^2)}$$

n – sample size
n= Population size
e – Error (tolerable say 5%)

by putting e = 0.05 , e^2 = 0.0025
N=12996

$$n = \frac{12996}{1 + (12996 \text{ x } 0.0025)}$$

$$= \frac{12996}{33.49}$$

n = 388.05

Sample size = 388

Figure 3.1 Formula for obtaining sample size

3.12. Data collection methods

Data collection is the method of gathering data from all available sources in order to solve the study issue, test the hypothesis, and assess the results. Data collection methods are classified into two categories: secondary data collection methods and primary data collection methods.

3.12.1. Primary data

Primary data is collected through survey questionnaire. This data is first hand and completely unique. Data may be collected in a number of ways, including observation, experiment, questionnaire discussions case studies, Interviews and focus groups. However the most popular data collection techniques are questionnaires and interviews. In this research the data is collected by sending online questionnaires using Google form and the respondents were asked to fill them out. Interview based manual method of data collection is also used.

3.12.2. Secondary data

When a researcher uses secondary data, he may possibly look into a variety of sources in order to obtain it. Secondary data is research information that has already been collected and is available to researchers. Primary data, on the other hand is exactly opposite of this as this data is extracted from direct sources (C.R.Kothari.). Secondary data is useful and powerful source of information. The main advantages of secondary data is due to Internet it is available in ample, easily accessible, low cast or no cost and time saving.

Generally published data can be accessible from:

- Internet/ Web information
- Publications of the central, state are local governments
- Publications of foreign governments
- Official trade journals
- Books, magazines and newspapers
- Reports and publications of various associations connected and industry
- Reports prepared by research scholars, universities

- Public records and statistics, historical documents, and other sources of published information.

There are many sources of unpublished data. They can be found in diaries, correspondence, unpublished biographies, and autobiographies, as well as with academics and researchers, trade unions, labour bureaus, and other public and private people and organisations.

As discussed, secondary data might be seen as a very good source for finding the factors affecting the privacy & security of smart home environment. Author has used Google scholar, Research Gate, Academia.edu to search the related material, and information related to this research.

3.13. Scale of measurement

In statistical analysis, the type of data/information given in numbers is referred to as the measurement scale. Each of the four scales (nominal, ordinal, interval, and ratio) provides information in a different way. Measurement is the process of assigning numbers to persons, items, and events in a meaningful way. Knowing how to perceive the numbers assigned to publics, substances, and events requires an awareness of measurement scales.

To conduct statistical calculations, it is necessary to understand variables and what should be measured using these variables. In statistics, there are various levels of measurement, and the data collected using them can be broadly classified as qualitative or quantitative. The type of statistical test to be used is determined by the level of measurement of a variable. The mathematical nature of a variable, or how a variable is measured, is referred to as its level of measurement. The three fundamental levels of measurement scales that are used to collect data in the form of surveys and questionnaires, each being a multiple choice questions, are described as Nominal, Ordinal, and Scale.

Nominal - A nominal scale is a naming scale in which variables are simply "called" or "labelled," with no particular order in mind.

Ordinal - The variables on an ordinal scale are arranged in a fixed order.

Scale – respondents to indicate their level of agreement, approval or, belief.

3.13.1. Survey questionnaire and its data type

SN	Questions From Questionnaire	Type of responses		
		Nominal	Ordinal	Scale
3	Age		Yes	
4	Gender	Yes		
5	Educational Qualification	Yes		
6	Employment status	Yes		
7	Monthly Income		Yes	
8	Since how long you have been using Smart Home?		Yes	
9	Application areas of Smart Home Devices	Yes		
10	Select the Smart Gadgets you use	Yes		
Authentication				
11	Data authenticity in relation with authenticated devices			Yes
12	Sharing data with third party for advisement			Yes
13	Data sharing with relatives / care taker			Yes
14	Disabling security authentication under emergency condition			Yes
Authorisation & access control				
15	Allowing government agencies to use information generated by smart home			Yes
16	Allowing government agencies to allow data access in case of casualties (Fire brigade)			Yes
17	Allowing Law enforcement agencies to access data during crime investigation			Yes
18	Need to offer role based system for guest			Yes
19	Configuring Wi-Fi / Bluetooth high level of security			Yes
Confidentiality				
20	Feeling safe storing personal / family confidential information on smart home system			Yes
21	Possibility of Privacy violation when one can’t control how much data is collected by smart devices (e.g. Google assistant)			Yes
Integrity				
22	Trust on data stored in encrypted form			Yes
23	Device verification to ensure reliability of data source			Yes

SN	Questions From Questionnaire	Type of responses		
Availability of asset/devices				
24	Reputational loss due to leakage of sensitive data/information			Yes
25	Necessity to keep devices at secure place			Yes
26	Unresponsive security of smart home devices			Yes
Ease-of-use & cost				
27	Is ease of use preferred over smart home security considerations?			Yes
28	Does security measures reduces user friendliness			Yes
29	Is cost of automation more important than smart home security considerations			Yes
Accountability				
30	Necessity of system security updates reviewed from time to time (from smart home device manufacturer)			Yes
31	Getting real-time notification in case of device malfunction?			Yes
32	System should send alerts in case of data modification / alteration			Yes
33	User should get a real-time warning if an anomaly in smart home environment is detected			Yes
Trust				
34	Trust on security of doing online /financial transactions using smart home ecosystem(e.g. hacking of Wi-Fi)			Yes
35	Prefer branded manufactured products over local manufacturers			Yes
36	Smart home must provide privacy and security			Yes
37	Necessity of having essential built in security features by smart home device manufacturer			Yes
38	Need to have strict laws to protect individual privacy			Yes
Risk awareness/ Human factors				
39	Smart home safety and security are the main concern for implementing smart home system			Yes
40	Leak of smart home data/information can lead to unthinkable damages			Yes
41	Identity theft is the greatest risk against privacy for carrying out criminal activities			Yes

SN	Questions From Questionnaire	Type of responses		
42	Violation of smart home user's privacy may result into financial losses			Yes
43	It is necessary to avoid public Wi-Fi for remote access of smart home system			Yes
44	Unauthorized access of smart home system by hackers is the most critical security threat			Yes
45	Raising security awareness among users is essential for protecting smart home system			Yes
46	Smart home users carelessness or negligence in using the system is as dangerous as system being exposed to hackers			Yes
47	Knowledge on underlying technology to protect data theft from potential hacking is must			Yes

Table 3.3 Questionnaire and its typology

3.14. Questionnaire formation

The survey questionnaire is designed to analyse the user's awareness on smart home privacy and security against the threats which exist in smart home environment, users trust and confidentiality issues. Respondents are given a survey questionnaire covering all aspects of the objectives set in the beginning. There were total 47 questions in the survey form for collecting general demographic data as well as factors related to privacy and security issues in smart home environment. Respondents are asked to rate the factors using five-point Likert scale (1 being "Strongly disagree, and 5 being "Strongly agree"). To make task simpler for respondents, all of the questions were structured in a simple and direct manner. Detailed demography of questions given in the survey questionnaire is given below:

Question Number	Details	Remarks
1-10	Demographic questions	Questions related to the background of respondents
11-14	Authentication factors	Recognising user identity/Users privacy
15-19	Authorisation and access control factors	Question related to access rights/privileges to resources related to security
20-21	Confidentiality factors	Preventing users information from sharing or disclosure to the third party
22-23	Integrity factors	Question related correctness,

		completeness and loyalty
24-26	Availability of assets and devices factors	Availability is the assurance that systems and data are accessible by authorized users when needed
27-29	Factors related to ease of use and cost	Question related to user friendliness and cost effectiveness for security solutions
30-33	Accountability factors	Question related to obligation to accept the responsibility
34-38	Factors for Trust	Question related to trust on device manufacture / Internet
39-47	Risk awareness and human factors	Question related to risk awareness and awareness related to privacy & security concerns

Table 3.4 Detailed demography of survey questionnaire

Survey questionnaire was prepared using the factors present in Table 3.4 above. Google form was used to circulate survey questionnaire electronically to the respondents in order to understand the degree to which they agree or disagree on smart home privacy and security related factors (Briony Oates, 2006).

Five point Likert scale was used to get the responses from home users.

1 - Strongly Disagree

2 - Disagree

3 - Neutral

4 - Agree

5 - Strongly Agree

For collecting the response of survey questionnaire, author visited prominent housing societies where smart home users have dense presence.

Amanora in Hadapsar, Palladium in Kothrud, Jayashree society near Dandekar Bridge, etc are some of the housing societies to name a few.

3.15. Pilot research

In every research of larger scale the significance of pilot survey is immense. Pilot survey is in fact the replica (exact copy) and trial run of the main research survey. Such a survey being conducted by the researcher bring to the light the weaknesses/ limitation, if any of the questionnaires and also the survey techniques. Pilot trials are mini versions of full scale studies, also known as 'feasibility' study, as well as detailed pre-testing of a specific research instrument such as a questionnaire or interview schedule (Ranjit Kumar 2011). The size and design of the pilot survey is a matter of convenience. The sample of the pilot survey must be widespread as the main sample. All the techniques of processing and analysis of data have to be piloted. The pilot study is thus the researcher's last line of defence against the risk that the main study will be effective. Pilot survey is valuable if the main survey is too long and too expensive.

There is no clear definition on number of questions required for the pilot study. Generally pilot study sample size is considered 10% of the sample size used for main study, e.g. if sample size for main study is 500 then the sample size of 50 is reasonable enough.

In this research, the survey questionnaire was distributed to 38 users for pilot study. Users were mainly professionals mostly from interest community, students and woman. The term reliability and validity is used to assess the consistency of the questions in the survey questionnaire. They describe the accuracy of which a procedure, methodology, or tests something. Validity is concerned with a measure's precision, while reliability is concerned with its consistency. The questionnaire was evaluated with the Cronbach’s alpha and the test on confidence level. This procedure was used to understand whether the questions were clear to the respondents, whether they were in the right order, they describe the topic under study, the direction and whether any questions needed to be added or dropped.

The questionnaire was revised and expanded based on the findings. Final questionnaire was prepared for distribution in two forms- Google form for electronic circulation and printed form for manual data collection.

3.16. Reliability and validity test of Questionnaire:

a) Reliability of questionnaire using Cronbach’s alpha test

Reliability was measured using Cronbach alpha test. The reliability coefficient between 0.6 – 0.7 is considered acceptable.

- below .60 unacceptable
- between .60 and .65 undesirable
- between .65 and .70 minimally acceptable
- between .70 and .80 respectable
- between .80 and .90 very good

Reliability Statistics		
Cronbach's Alpha	**Cronbach's Alpha Based on Standardized Items**	**No of Items**
0.817	0.845	38

Table 3.5 Reliability statistics

b) Validation of questionnaire after discussion with domain expert

The accuracy with which a system calculates what it is supposed to calculate is referred to as validity. When study has a high level of validity, it provides findings that correlate to real-world properties, features, and variations. The Questionnaire being used was well structured to determine the preciseness and reliability in the course of the study. The research questionnaire validity was determined by having the discussion of experts in the field, especially security experts.

3.17. Research Hypothesis

A research hypothesis (or scientific hypothesis) is an assumption of the expected relationship between variables or an interpretation of the occurrence, which is straightforward, precise, testable and verifiable. Hypothesis is framed by the researcher on the basis of knowledge acquired through literature review, existing models, frameworks, proven theories, etc. The hypothesis framed is then validated using appropriate statistical technique and statistic value.

For this research, author has framed three hypotheses. These hypotheses will address the objective set in the beginning of research.

H1: Smart home users are not fully aware about the data security features of smart home devices.

H2: Smart homes environment are significantly vulnerable to hackers if not configured properly

H3: Security awareness is directly related to an appropriate access control of smart home system.

3.17.1. The table below summarises the association between the hypotheses and objectives, as well as related elements in the questionnaire.

Objective	Hypothesis	Question in the questionnaire
O1: To identify the dimensions of privacy and security pertinent to smart home environment.	**H1:** Smart home users are not fully aware about the data security features of smart home devices **H2:** Smart homes environment are significantly vulnerable to hackers if not configured properly	**14.** Do you agree that under emergency, it is OK to disable security authentications? **18.** Do you believe there is a need to offer separate role based management and operational authentication for guests? **19.** Do you feel your wi-fi / bluetooth should be configured to high level of security **20.** I don't feel safe storing personal / family confidential information on smart home system **23.** I think "Device verification" is must to ensure reliability of data source **26.** I feel worried about unresponsive security devices **27.** Is ease of use preferred over security considerations? **36.** I think I can ensure my smart home environment privacy and security **39.** I think home safety and security are main concern for implementing smart home system **44.** Do you agree that unauthorized access to system, virus / worm, denial of service attacks are most critical security threats to your smart home system? **47.** Do you agree that user should understand the underlying technology to protect from potential

Objective	Hypothesis	Question in the questionnaire
		hacking / data theft?
O2: To study the impact of significant factors on smart home privacy and security.	**H2:** Smart homes environment are significantly vulnerable to hackers if not configured properly **H3:** Security awareness is directly related to an appropriate access control of smart home system	**21.**I think privacy is violated when one cannot control how much information is collected by smart devices (e.g. possible storage of all conversations on Alexa / Google assistant) **22.** I believe "Data stored in Encrypted" form cannot be altered/ modified **24.** I feel loss of sensitive information can cause lot more harm and damage like Reputational loss. **25.** Do you feel it is necessary to keep devices at secure place to prevent device theft / Damage? **28.** Do you think a Security measure reduces under friendliness? **29.** Is cost of smart home device and automation services more important than security considerations? **34.** I don't feel comfortable doing online /financial transactions due to security reasons (e.g. hacking of Wi-Fi) **40.** I believe losses, incurred due to information leak can lead to unthinkable damages **41.** I Consider Identity theft is a greatest risk against privacy? (e.g. misused in criminal activities) **42.** I feel violation of user's privacy may result into financial losses **43.** I feel it is necessary to avoid public wi-fi for remote data access to home system.

Objective	Hypothesis	Question in the questionnaire
O3: To perform critical assessment of security vulnerabilities inside and outside the smart home environment	**H3:** Security awareness is directly related to an appropriate access control of smart home system	**11.** I feel it is necessary to check whether the information is coming from authenticated devices **12.** I feel information generated by smart devices should not be shared or used by 3rd party (i.e. advertising / sales) **13.** I would not mind if my health data is shared with my caretaker/ friends / relatives /research organizations **15.** If given a choice would you say YES to government agencies for collecting/ using the data/information generated by smart home system? **16.** It is OK to allow government agencies to give access in case of casualties (for e.g. Fire brigade) **17.** I would prefer to allow law enforcement agencies to access my smart home related data for crime investigation? **34.** I don’t feel comfortable doing online /financial transactions due to security purpose (e.g. hacking of Wi-Fi) **35.** I prefer branded manufactured products over local manufacturers **46.** I strongly feel careless or negligent smart home users are as dangerous as hackers
O4: To develop an optimal and dynamic conceptual framework of smart home ecosystem to mitigate privacy and security	Experimentation based conceptual framework **Safe@Smarthome** is proposed by the author. This framework is validated using Case Based Research (CBR) approach (see Data Analysis chapter-4 for detail).	

Objective	Hypothesis	Question in the questionnaire
related threats/risks issues in smart homes		
O5: To provide recommendations for the betterment of privacy and security of smart home users data (big data)	**H1:** Smart home users are not fully aware about the data security features of smart home devices **H3:** Security awareness is directly related to an appropriate access control of smart home system	**30.** Do you feel smart home system's access should be reviewed from time to time (like password updates, security updates from manufacturer)? **31.** Do you think you should get a real-time notification in case of device malfunction? **32.** I Expect my smart home system should send alerts in case of data modification / alteration **33.** Do you think you should get a real-time warning if an anomaly in the home environment is detected? **37.** I think it is essential for companies which develop smart devices to provide built in security features **38.** Do you feel there should be strict laws to protect individual's privacy? **45.** Do you agree that "Raising consumer awareness regarding security of connected devices" is must for protecting smart home system

Table 3.6 Association between the objectives, hypotheses and research question

3.18. Data analysis tools and Techniques used

Different statistical techniques are used to check the statistical significance. Such statistical analyses also aid in the drawing of inferences and the formulation of recommendations. Whenever it comes to survey analysis, researchers must use quantitative data analysis techniques. IBM Statistical Package for Social Science

(SPSS) version 18 has been used for data analysis. The analysis can be descriptive in nature, allowing for the use of descriptive statistical methods such as percentile scores, charts, and tables to describe the sample. It can be inferential to test the hypotheses statistic.

Statistical tests used **in this research work include:**

- **Shapiro-Wilk test** – The Shapiro-Wilk test is a method of determining if a random sample is drawn from a normal distribution. A small W value indicates that the sample is non-normally distributed.
- **Kolmogorov-Smirnov (KS test)** – KS test is one of the most useful and general nonparametric statistical test for comparing two samples.
- **Chi-square test** – The chi-square independence test is a method for determining whether two categorical variables in a population are correlated.
- **Spearman–correlation test** – Spearman's correlation coefficient is a statistical tool for determining the statistical association, or relationship, between two or more variables. It provides information on the extent and direction of the relationship's association, or correlation.
- **Cronbach's alpha test** – Also named as Coefficient test, measures reliability, or internal consistency. “Reliability” is another name for consistency.

3.19. Ethical considerations

One of the most critical aspects of the research is the ethical issues. If this component is missing, dissertation is challenged. In order to adequately confer the ethical considerations part of research following are the few points that need to be considered (Broney oates , 2011).

- Respondents' privacy and anonymity are of utmost importance.
- The confidentiality of the study data should be maintained to an adequate degree.
- Prior to the study, the participants' full consent should be obtained.
- Respondents' willingness to participate in the study is important. Furthermore, participants have the option to withdraw from the study at any time if they so choose.

- Respondents should give their informed consent to participate. The theory of informed consent entails researchers providing adequate information and guarantees about participating in order for individuals to fully understand the consequences of participation and to make a fully informed, considered, and freely provided decision whether or not to participate, without any pressure or influence.

As the objective of this study is privacy and security assessment of smart home users, the privacy of respondents is taken care of during the process of collecting the response. The respondents were informed that their identities will not be disclosed in any case. Even in few cases the right of not to participate and right to withdraw is also agreed.

3.20. Methodology Limitations

While performing online survey, the author encountered the following challenges:

1. Insensible respondents - Respondents are reluctant to fill the questionnaire
2. Dishonest answers - Many respondents were unenthusiastic towards filling the questionnaire. Particularly those who were unfamiliar to the researcher.
3. Skipped questions - Quite a few respondents did not completed the entire questionnaire, leading to reduced response rate.
4. Time consuming - Questionnaire method is more time consuming.
5. Confidentiality - The participant might be unable to reveal such private details, which may negatively impact the outcomes.
6. Misinterpretation - Without someone to thoroughly clarify the questionnaire and ensure that everyone understands it, the findings may be arbitrary.

3.21. Conclusion

This chapter describes in detail about the research methodology adopted in this research. The chapter discussed different research paradigms and methodologies, as well as justifying the research design and methodology. The methods of data collection, data interpretation, and ethical considerations were all discussed in detail. In this study, survey through a Google form and hard printed manual questionnaire was used for data collection. The questionnaire had two sections: General for demographic data and Likert scale based factors data on smart home privacy and security related data for inferential analysis. A five-point Likert scale was selected to measure responses to each item in the attitude measurement questions which were based on the literature. The descriptive and inferential statistics were produced using the IBM SPSS 18.0 statistical package. Five statistical analysis tests- Shapiro-Wilk test, Kolmogorov-Smirnov, Chi-square test, Spearman–correlation test, Cronbach's alpha test were used to obtain the research output.

CHAPTER 4 - DATA ANALYSIS & INTERPRETATION

CHAPTER 4

DATA ANALYSIS & INTERPRETATION

4.1. Introduction

This research aims at assessing the privacy and security in smart home environment. In this research author has not applied big data analytics or have used any tools and/or techniques related to big data anywhere, but, those smart home devices that are generating big data and upon which big data analytics is applied by the service provider for better user experience are focussed.

In order to complete the research objective, data is collected from smart home users from across Pune region. Questionnaire based electronic survey forms, manual forms and interviews were used as a data collection tool.

After rigorous literature reviews and research gap analysis, factors related to smart home security and privacy were identified. Author has identified and included those factors which are mentioned in the literatures reviewed on the subject. Author has included those factors where the researchers had carried out proper confirmatory test for its validity. The numbers of factors identified from such literary works comes out to be 50. But, since the numbers of smart home users are limited and their types are varied it was very difficult to converge on the valid factors to start the research. Author has therefore conducted a pilot survey among closed group of identified smart home users and smart home related service providers. After a pilot study, 37 factors out of total 50 were found to be most important and valid. These 37 identified factors are finally included in the research questionnaire.

Final research questionnaire carries total 47 questions, 10 are general questions about respondents and 37 questions are ranking scale questions to assess the privacy and security of smart home environment.

In order to meet the research objective, author has proposed 3 hypothesis covering entire 37 valid identified factors.

Data analysis employs use of statistical techniques and graphical tools to extract information from the data collected for the research.

Total responses received through manual/electronic survey and interviews were 400 plus out of which 396 responses complete in all respect is used in the analysis of result.

Entire research is carried out in 3 phases as below:

Phase-1: Validating the research hypothesis.

Phase-2: Proposing a conceptual framework "Safe@Smarthome" for smart home Privacy and Security.

Phase-3: Validating the proposed framework using case based approach.

This chapter begins with an analysis of questionnaire responses. This will explain the rationale, such as:

- What are the most popular smart home devices among smart home users?
- Are smart home users conscious about their personal data which gets shared while using smart home devices?
- While using smart home devices are users willing to share their private information?
- What is the general level of security awareness among smart home users?
- Do consumers have any concerns about data storage and device security?
- What are users' security perceptions?
- What suggestions are needed on emerging solutions to improve their usability and usefulness?

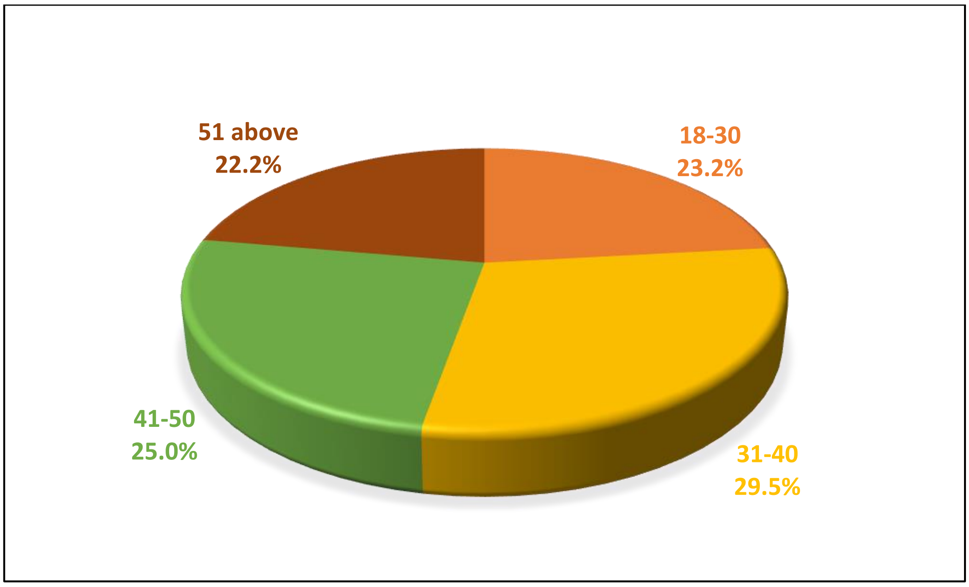
4.2. Descriptive statistics

1. Age of the respondent

Age is the demographic factors that influence the usage of the modern technology. For the proposed research, age of the respondents is categorised into four distinct types and it is shown in the below table.

Age of Respondents	Frequency	Percent
18-30	92	23.2%
31-40	117	29.5%
41-50	99	25%
51 above	88	22.2%
Total	396	100%

Table 4.1 Age of the respondents



Graph 4.1 Age of the respondents

Observations:

It is found that out of 396 respondents 23.2% belongs to 18-30 years age group, 29.7% belongs to 31-40 years age group, 25.1% belongs to 41-50 years age group and 22.2% belongs to above 51 years age group.

Inference:

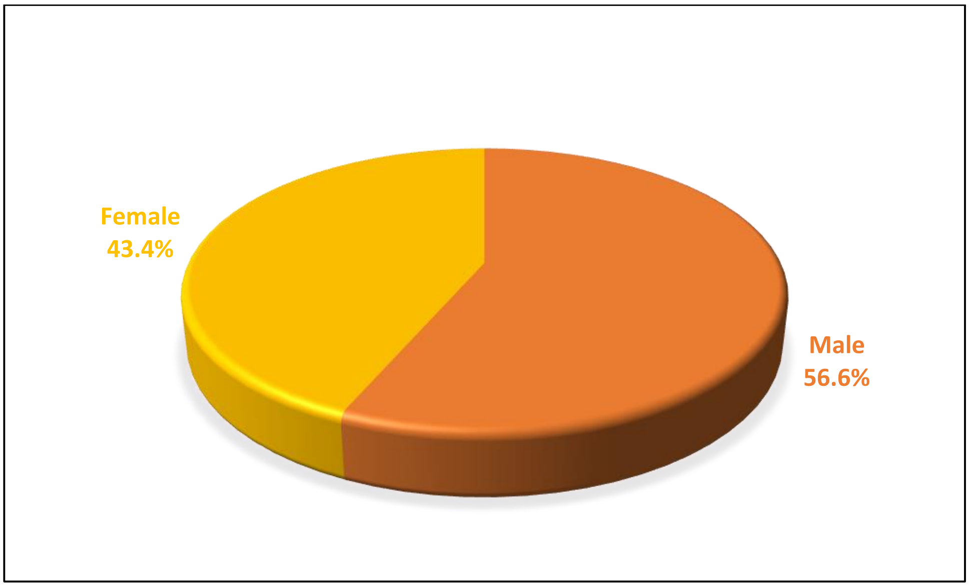
Responses received are evenly distributed among all age group and is following a Gaussian distribution. Highest percent of smart home users i.e., 54.8% belongs to middle age group 31-50 years. Most of the smart home devices are managed by middle age members in a family.

2. Gender category

Respondents were asked to fill their gender. This helps in understanding gender biasness among smart home users. For capturing the response three categories were given:

Gender	Frequency	Percent
Male	224	56.6%
Female	172	43.4%
Total	396	100%

Table 4.2 Gender of the respondents



Graph 4.2 Gender of the respondents

Observations:

Out of 396 respondents 56.6% respondents are males and 43.4% are females**.**

Inference:

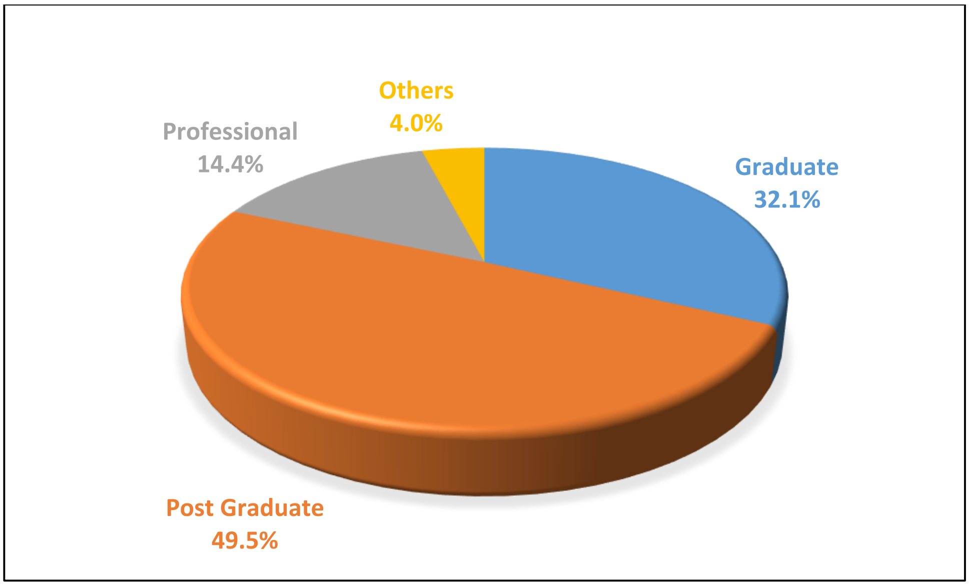
The responses received from males are 13.2% more than by the females. This difference is justifiable considering the male is to female ratio of 1000:929 in Maharashtra. Including this fact, gender biasness is not there among the respondents of smart home device.

3. Educational Qualification of the respondents

The Educational Qualification is asked to understand what role qualification contributes in using smart home devices.

Responses	Frequency	Percent
Graduate	127	32.1%
Post Graduate	196	49.5%
Professional	57	14.4%
Others	16	4.0%
Total	396	100

Table 4.3 Educational qualifications of the respondents



Graph 4.3 Educational qualifications of the respondents

Observations:

The table shows that 32.1% respondents holds a Graduate degree, 49.5% holds post Graduate, 14.4% respondents have a Professional qualification and 4% have qualification other than the listed.

Inference:

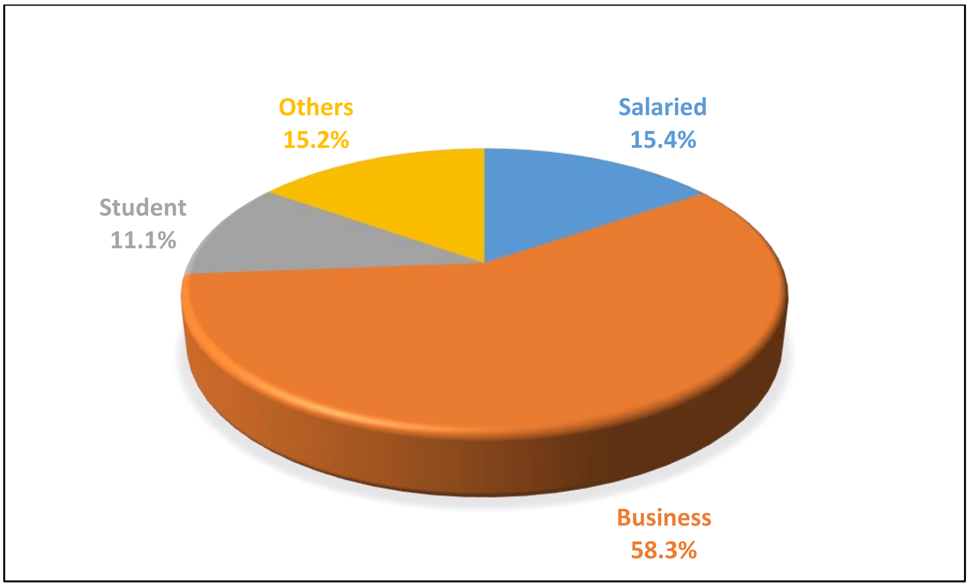
As the research is conducted in urban background, the maximum number of respondents are having qualification graduate and above. Only 16% of the respondents possess below graduation level qualification. Thus, education has influence on the usage of smart home devices; it plays an important role in the use of emerging technology.

4. Employment status

Smart home solutions are expensive and the past researches conducted on the area suggest the use of IT/ITES is related to the employment status. Like, a business class prefer to use gadgets/devices more for safety and security over a normal salaried class. In order to understand the same author has asked a question on employment status. Respondents are asked to choose the employment status from Salaried, Business, Student or others.

Employment status	Frequency	Percent
Salaried	61	15.4%
Business	231	58.3%
Student	44	11.1%
Others	60	15.2%
Total	396	100%

Table 4.4 Employment status of respondents



Graph 4.4 Employment Status of respondents

Observations:

Respondents from all the occupational segments of the society are investigated. Highest numbers of response i.e., 58.3% are business class, 15.4% are salaried, 11.1% are students and 15.2% are others (this includes housewives).

Inference:

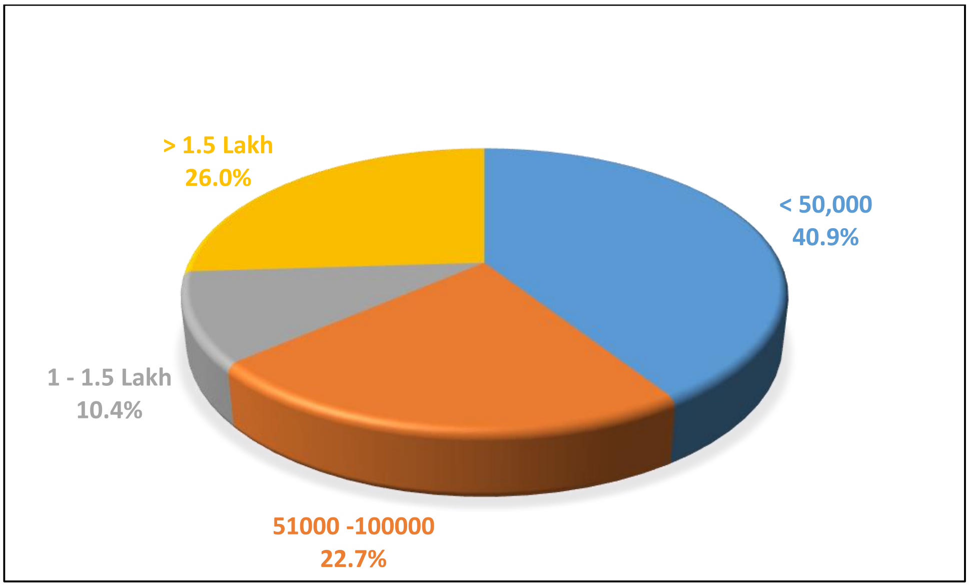
Business class prefer using smart home system. The reason as cited by past researchers includes- their ability to spend on expensive solution and vulnerability from thefts and home security. Though author has conducted any direct survey on this fact but, literature review carried out during this research has surfaced this fact. In this research it holds true.

5. Monthly Incomes of respondents

Expense made in smart home devices is linked to income of user. Higher the income, higher could be the usage of smart devices. The availability of funds would, of course, lead to distribution of funds to different forms of spending on needs. The purpose of this question is to understand how far the respondents' income represents the utilisation in smart home devices.

Monthly Income	Frequency	Percent
< 50,000	162	40.9%
51000 -100000	90	22.7%
1 - 1.5 Lakh	41	10.4%
> 1.5 Lakh	103	26.0%
Total	**396**	**100%**

Graph 4.5 Monthly incomes of respondents



Graph 4.5 Monthly incomes of respondents

Observations:

Respondents' average monthly income is classified into 5 categories. Majority of the respondents are in the monthly income bracket of less than Rs. 50,000 i.e. 40.9%, 22.7%

have income bracket in the range Rs. 51000 to 1 Lakh, 10.4% lies in the bracket of Rs. 1 Lakh to Rs.1.5 Lakh and 23.5% respondents lies in the bracket greater than Rs.1.5 lakh.

Inference:

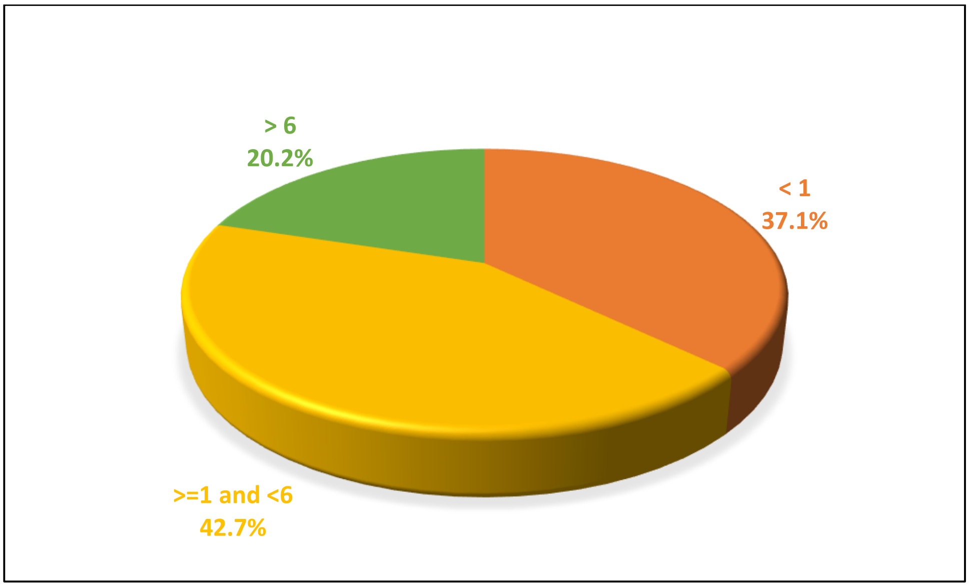
Out of the total 386 complete response for this question, 58% of the respondents are having monthly income higher than Rs. 51000/-. Therefore, the majority of smear home device users comes from Higher Middle class family.

6. How long you have been using Smart Home device

Respondents were asked to record since how many years they are using smart home device. Responses received are present in table 4.6 below.

Usage of smart devices	Frequency	Percent
< 1	147	37.1%
01- 06	169	42.7%
> 6	80	20.2%
Total	396	100%

Table 4.6 Respondents experience in using Smart Home device



Graph 4.6 Respondents experience in using Smart Home device

Observations:

Out of the total 397 respondents, 42.7% are using smart home devices from 1 to 6 years, 37.1% respondents are using since last 1 year and only 20.2% respondents are using smart home devices for more than 6 years.

Inference:

Mature users (experience greater than 6 years) occupy only 20.2% of the total sample. This shows that the concept of smart home is relatively new in India. The next major chunk of 42.7% goes to the users using smart home devices between 1 to 6 years, this is again indicator of upward trends.

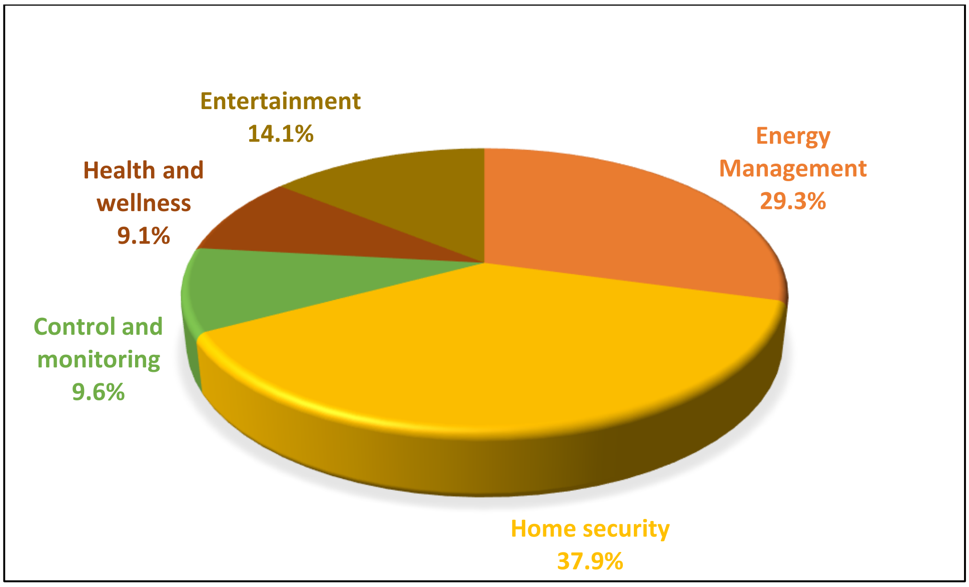
7. Application areas of Smart Home Devices

There are varieties of smart home devices and so are applications available for smart home users. The types of services availed by the users are increasing day-by-day. Instead of going to an individual device/application, author has categorised them into 5 classes.

The table below displays various application areas of smart home. The most popular applications is home automation that controls the lighting, HVAC, Entertainment, kitchen appliances and security systems. The list is growing every day.

Responses	Frequency	Percent
Energy Management	116	29.3%
Home security	150	37.87%
Control and monitoring	38	9.6%
Health and wellness	36	9.1%
Entertainment	56	14.1%
Total	**396**	100%

Table 4.7 Application areas of Smart Home Devices



Graph 4.7 Application areas of Smart home users

Observations:

The table shows different application areas in smart home environment. Out of 390 completed responses maximum respondents (66.7%) are interested to use smart home application for energy management and home security. 36.4% respondents have agreed to use smart home device for security applications. Health and wellness accounts for after that 14.1% user opted entertainment

Inference:

Data suggests that maximum users (36.4%) prefer using smart home application for home security. Energy conservation is another concern that accounts to 29.3%. Other uses accounts to a very small 33.3%. The result is indicating that the smart home application preferred by the respondents requires use of big data analytics.

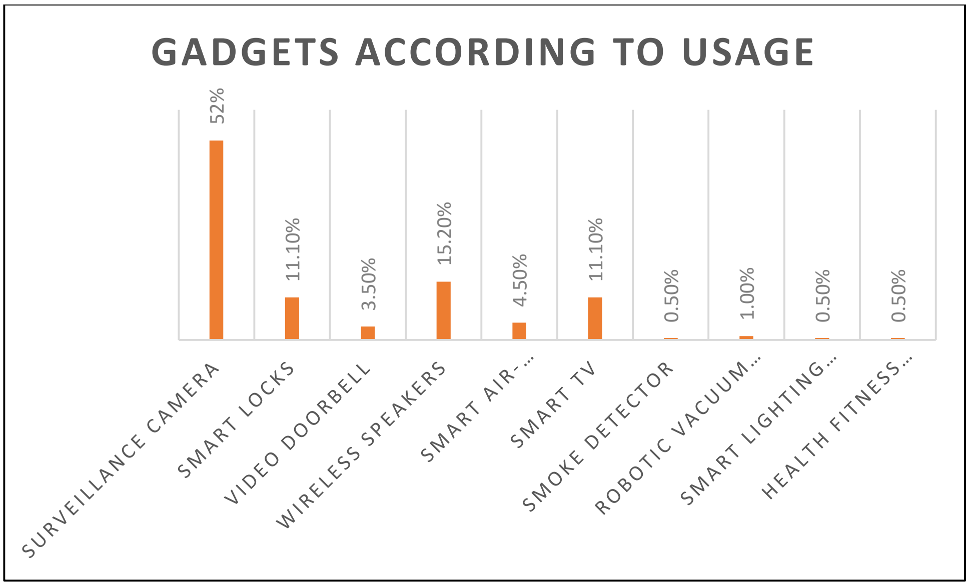
8. Distribution of smart home devices according to usage

Once the application areas are identified it is equally important to study what are the different types of devices or gadgets used by various smart home users.

Respondents are asked to specify which smart home device or gadget they use in smart home application they are using, for example surveillance camera (CCTV), smart TV, wireless speakers- Alexa, Amazon Echo etc. Table below shows the distribution of smart home device/gadgets respondents were using.

Responses	Frequency	Percent
Surveillance camera	206	52%
Smart locks	44	11.1%
Video doorbell	14	3.5%
Wireless speakers	60	15.2%
Smart air-conditioner	18	4.5%
Smart TV	44	11.1%
Smoke detector	2	0.5%
Robotic Vacuum cleaner	4	1.0%
Smart lighting control	2	0.5%
Health fitness devices	2	0.5%
Total	396	100%

Table 4.8 Distribution of smart home devices/gadgets according to usage



Graph 4.8 Distribution of smart home devices/gadgets according to usage

Observations:

Out of 392 complete responses 52% users are using Surveillance camera/ CCTV, 15.2% agreed of using wireless speakers and 11.1% users were using Smart TV and others accounts for 21.7% that includes smart locks, video doorbells and smart air-conditioning system collectively contributing to 19.1%.

Inference:

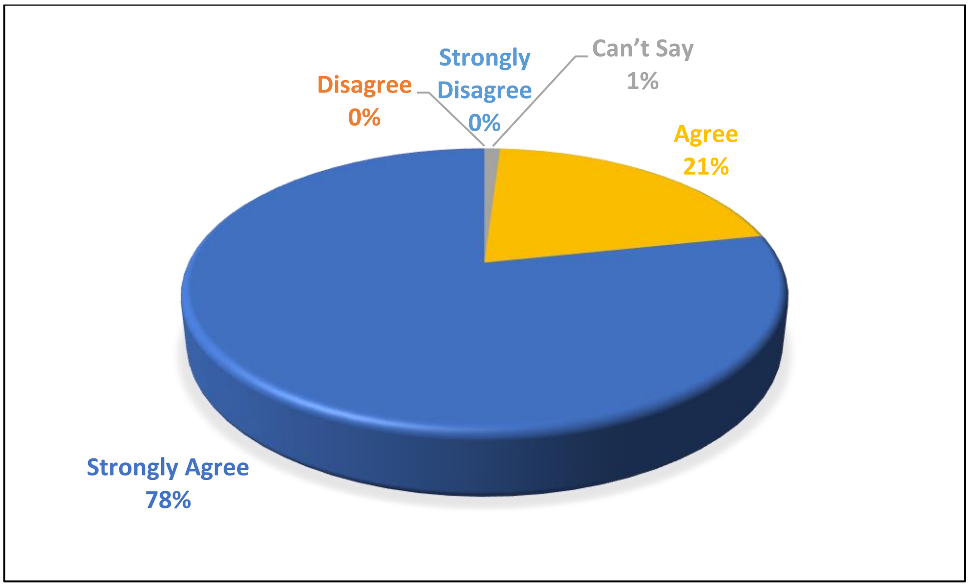
Data suggests that the major use of smart home devices/gadgets is for home security related applications. Use of connected CCTV cameras for surveillance, smart locks, connected video door bells, smart air-conditioning system and voice commands enabled wireless speakers collectively accounts to massive 87.2%. This is an indicator of use of smart home devices using big data analytics.

9. Data authentication in smart home device

Data authentication is a major concern and it accounts for security related issue. Smart home users are asked whether they know whether the data authentication mechanism is properly enabled in their smart home devices and they know whether data transmission is taking place through authenticated device. This response is important to know the users knowledge relating to security of smart home devices.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	0	0
Can't Say	4	1%
Agree	82	20.7%
Strongly Agree	310	78.2%
Total	396	100

Table 4.9 Data authentication in smart home device



Graph 4.9 Data authentication in smart home device

Observations:

Data suggests that majority of respondents (99 %) knows about data authentication in smart home devices and they believe it is important; minor 1% percent respondents were confused about smart home data authentication.

Inference:

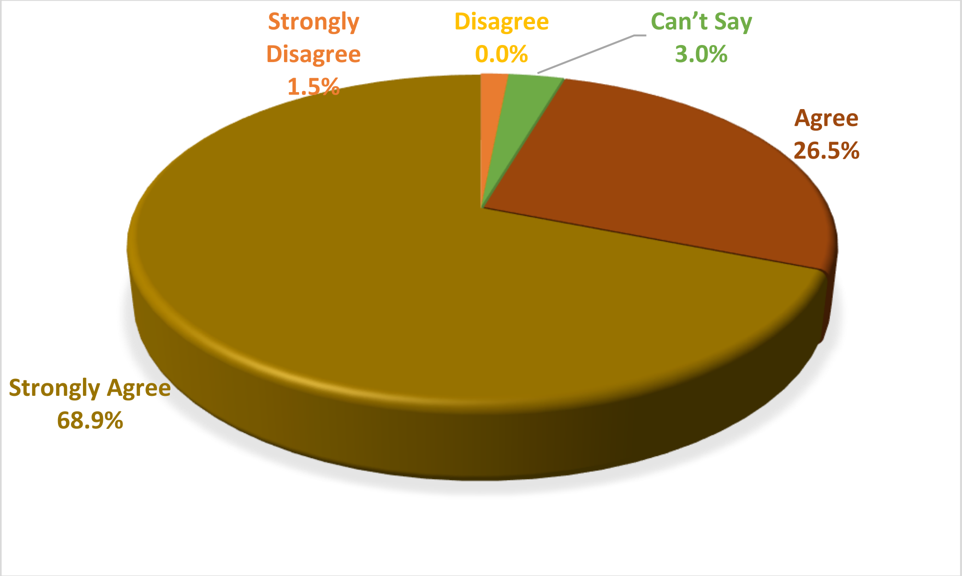
Smart home devices require proper internet connectivity. All the connected devices routes through the Wi-Fi enabled router switch. Thus, there are two levels of authentication- first at router level and another at device level. Author has collected the data related to users qualification and majority are having qualifications graduation and above. The responses received are in line with the fact that literate users have knowledge about authentication and this is confirmed by their responses and thus the result.

10. Do you think that the data generated by smart devices should not be shared or used by other parties (for example, advertising or sales)?

Smart home ecosystem requires lots of data generated through smart home devices to be collected and analysed using big data analytics to create pervasive or connected space. This requires collection of personal preferences related data. Such data is being processed at an exponential rate in today's connected world. However, personal data is very important; it is vulnerable to exploitation or misuse by unknown people without consent. Intrusion in the smart home ecosystem or sharing of data by service provider can be dangerous. The objective of this question is to know the user preference on the issue.

Responses	**Frequency**	**Percent**
Strongly Disagree	6	1.5%
Disagree	0	0
Can't Say	12	3%
Agree	105	26.5%
Strongly Agree	273	68.9%
Total	**396**	**100%**

Table 4.10 Smart home related data sharing with 3rd party



Graph 4.10 Smart home related data sharing with 3rd party

Observations:

Out of the total 396 responses received, 95.5% users agree that data should not be shared with 3rd part. A small (3%) of users were confused whereas 1.5% have consented on data sharing with 3rd party.

Inference:

The response again indicates that since most users are using smart home device for home security, therefore, any such breach of data may have a serious consequences. That is why 95.5% respondents agree that data should not be shared with 3rd party. The users that have agreed for the sharing i.e., 1.5% may be probably those who are using health related device/gadgets.

11. Users views on sharing data with Friends, relatives and research organizations

Under General Data Privacy Regulation (GDPR) act, sharing the personal data is prohibited without consent from the individual. So this question tries to understand the users awareness about the sharing the data with their closed contacts. Data breach can happen even it data theft takes from your closed acquaintances.

Responses	Frequency	Percent
Strongly Disagree	40	10.1%
Disagree	58	14.6%
Can’t say	72	18.2%
Agree	141	35.6%
Strongly agree	85	21.5%
Total	**396**	**100%**

Table 4.11 Users views on sharing data with Friends, relatives and research organization

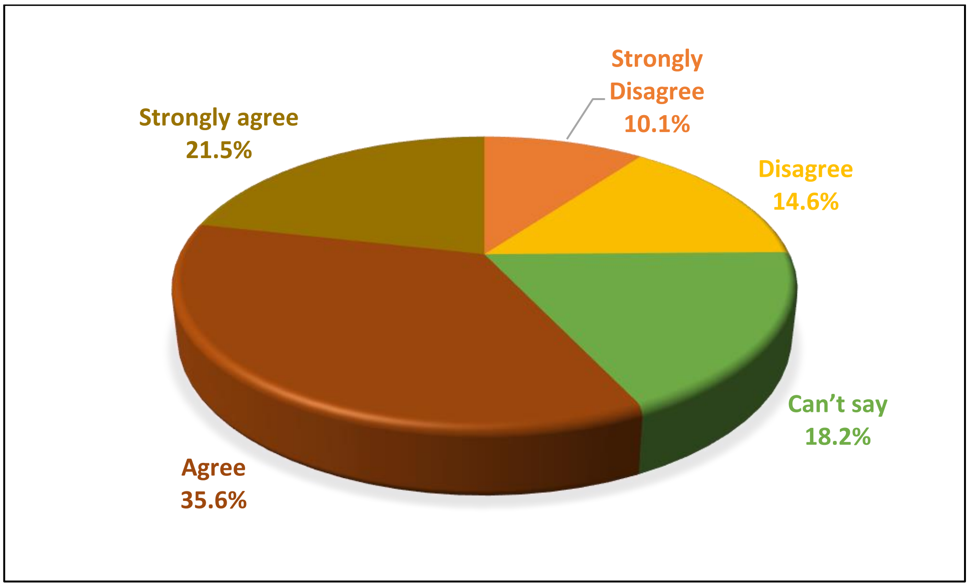


Table 4.11 Users views on sharing data with Friends, relatives and research organization

Observations:

From above graph & table near about 35.6% uses have agreed to share the data with their friends and relatives, 21. 5% users strongly agree that they can share the data with their friends and relatives, 18.2% users have neutral opinion and approximately 25% (24.7%) have shown their disagreement upon sharing data even with their friends and relatives.

Inferences:

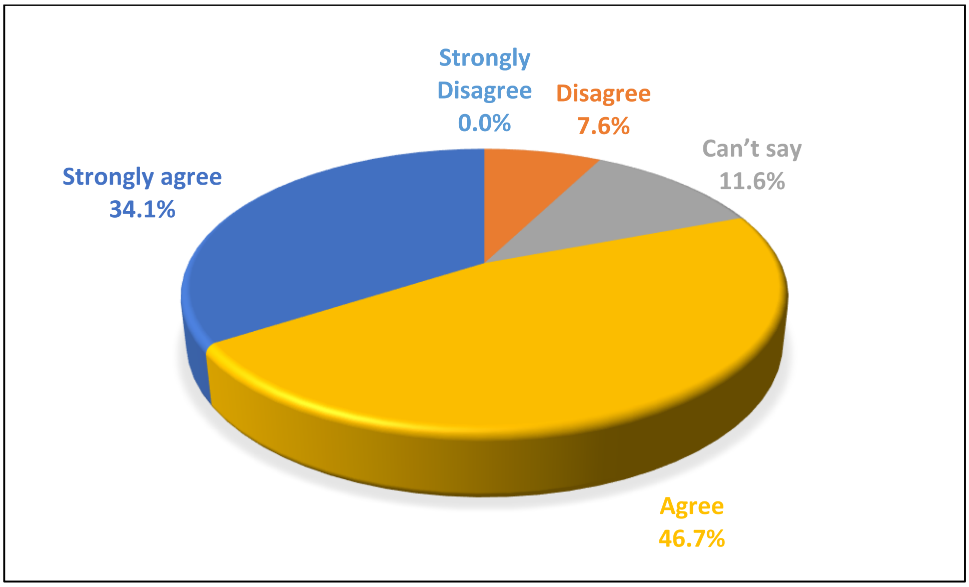
About 60 % of the users have responded they do not mind sharing the data with their friends, relatives and friends. This may be due to the fact that they are unaware of the GDPR Act and also may be ignorant about data breach through data sharing. About 40 % users that comes in the category of disagreement and unclear both probably are more aggressive regarding their personal data. Since author has not asked any question related to GDPR Act, it cannot be said whether those users who disagreed have any knowledge about the act, but most of the users are literate and are professionally qualified so this fact can be probable and cannot be ignored.

12. Do you think security authentication should be deactivated in an emergency situation?

The purpose of this question is to know users awareness about ill consequences during malicious security attack. As most of the users are smart home users, not deactivating the device and system may be dangerous and entire home security or device/gadgets control can be lost. The response will help to understand users action during emergency situation when devices and under attack.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	30	7.6%
Can't say	46	11.6%
Agree	185	46.7%
Strongly agree	135	34.1%
Total	396	100%

Table 4.12 Authentication deactivation in an emergency situation



Graph 4.12 Authentication deactivation in an emergency situation

Observations:

Responses reveal that more than 80% of the users are ready to deactivate their device authentication in an emergency situation (46.7% of the users are ready to compromise on their smart home device security authentication in an emergency situation whereas 34.1% strongly agree on this opinion). Only 19% of users comes under the class of unsure and disagree.

Inference:

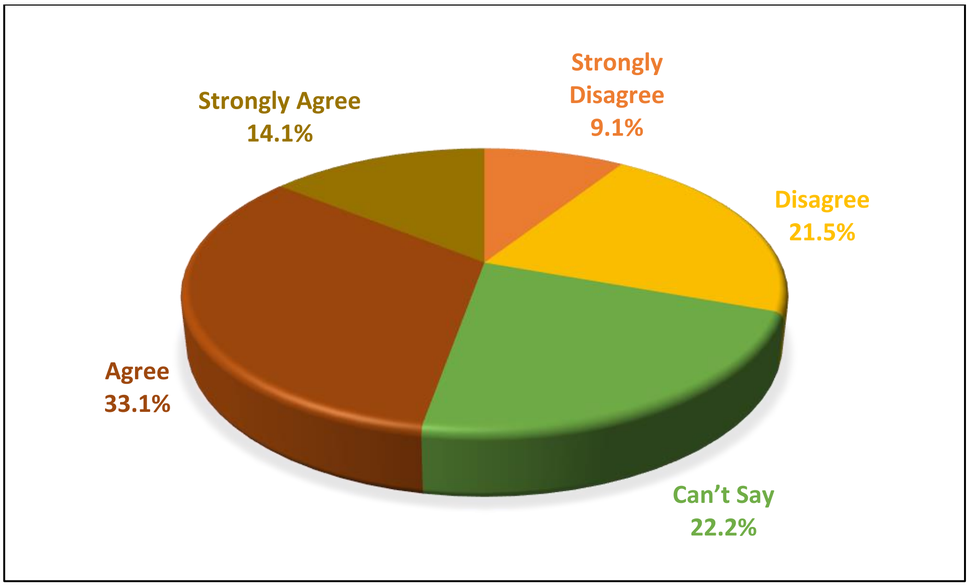
Massive users (80%) are aware that they need to deactivate their devices in an emergency situation.

13. Do you allow government agencies to collect and utilise the data collected by your smart home provider?

It is important to know whether smart home users allow access of their data for utilization by government agencies. This is data privacy related concern. This question tries to analyse whether respondents would like to share their personal information with Government agencies. This can be for the purpose of policy/strategy formulation by the government law making agencies.

Responses	Frequency	Percent
Strongly Disagree	36	9.1%
Disagree	85	21.5%
Can't Say	88	22.2%
Agree	131	33.1%
Strongly Agree	56	14.1%
Total	396	100%

Table 4.13 Data sharing with Government agencies



Graph 4.13 Data sharing with Government agencies

Observations:

Out of total 394 responses approximately 47% (46.9%) have agreed for data sharing with government agencies, 30.7% users do not want to share their personal data and 22.2% are not sure whether they should share their data with government or not.

Inference:

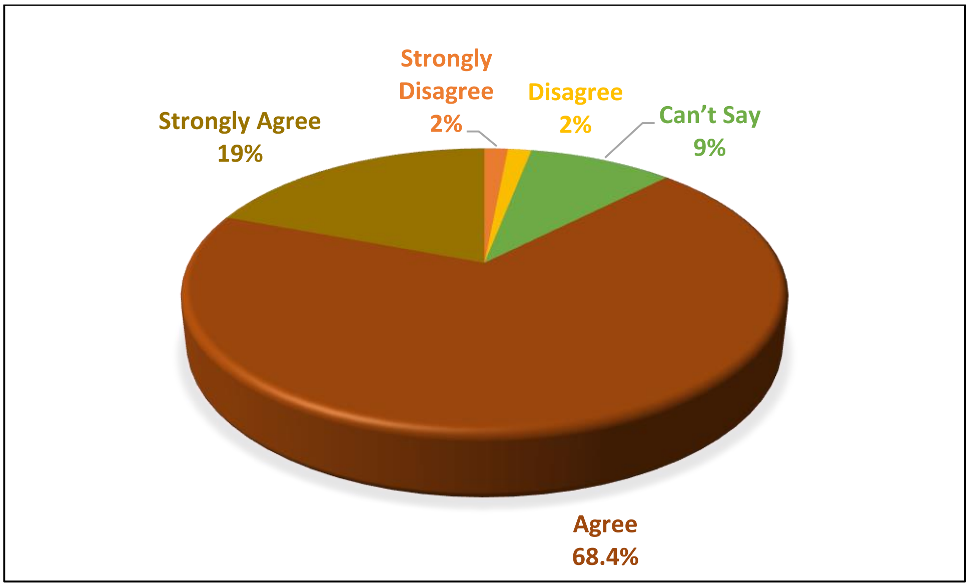
Smart home users are reluctant in their personal data sharing with government agencies. But, if the reason of data sharing is surfaced probably they would agree to share the data. The category of users who are unsure about data sharing accounts to 22.2%, this may get included with 46.9% users who consented for data sharing summing the total to 69.1%, provided the purpose is revealed. Sharing data with Government agencies becomes important in facilitating and enhancing public services.

14. Do you allow government agencies to access your data in the event of casualties (For e.g. Fire - brigade)?

Question number 13 and 14 are similar accept that in this question the purpose is to know the smart home users perception towards the data privacy and security during high emergency situation. This question is important to understand whether users are ready to compromise on data sharing during accidents/hazards or disasters.

Responses	Frequency	Percent
Strongly Disagree	6	1.5%
Disagree	6	1.5%
Can’t Say	37	9.3%
Agree	271	68.4%
Strongly Agree	76	19.2%
Total	**396**	100%

Table 4.14 Data access to government agencies in case of casualties



Graph 4.14 Data access to government agencies in case of casualties

Observations:

Out of total 390 responses received 68.4% smart home users agree to share data with government agencies in case of accidents/hazards or disasters, 19.2% strongly agree for data sharing, 7.8% were not sure and only 3% have shown their disagreement or are strongly disagree.

Inference:

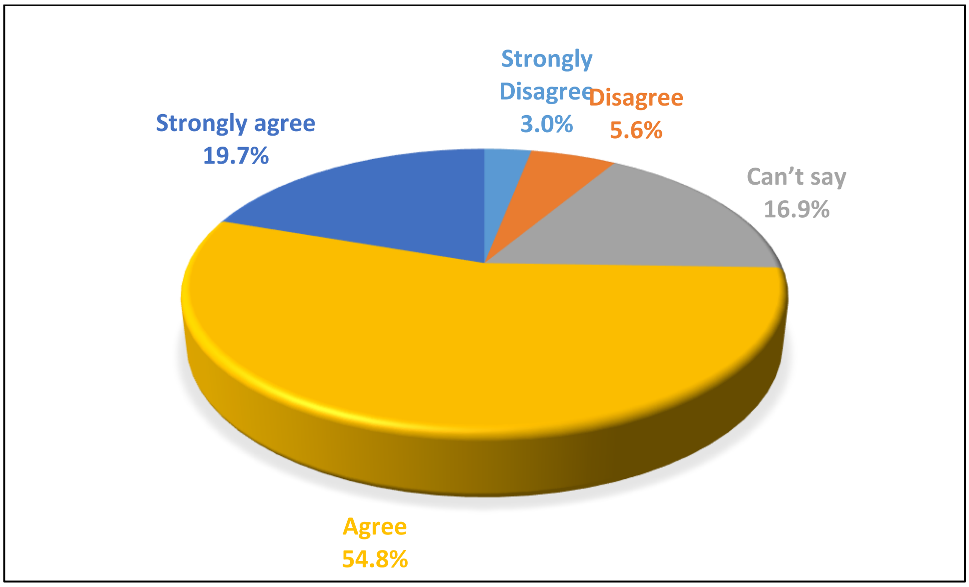
As is speculated in question no 13, where author has mentioned that the users may be ready to share the data provided the reasons are explained. It can be seen from the users response that 89% of users are agree to share the day with government agencies in the event of accidents/hazards or disasters. Only 3% of the users disagree, this may be due to proactive behaviour from data theft/misuse. It is worth noting that 7.9% are unsure about their course of action, this may be due to improper knowledge on smart device data management.

15. Do you allow law enforcement authorities to access your data for criminal investigation?

Past researches have revealed that crime investigation team collects the data from various sources to understand the modus operand of criminal and to crack it. This question is asked to know the users understanding on sharing their smart home data with government agencies which are into criminal investigation. The concern here is to know privacy issue of data.

Responses	Frequency	Percent
Strongly Disagree	12	3.0%
Disagree	22	5.6%
Can't say	67	16.9%
Agree	217	54.8%
Strongly agree	78	19.7%
Total	396	100%

Table 4.15 Data access by law enforcement agencies



Graph 4.15 Data access by law enforcement agencies

Observations:

Out of total 396 responses 74.5% respondents have agreed to allow data access to criminal

Investigating or government law enforcement agencies. Only 8.6% have shown their disagreement in sharing their smart home device related data whereas 16.9% were indecisive whether they should share the data or not.

Inference:

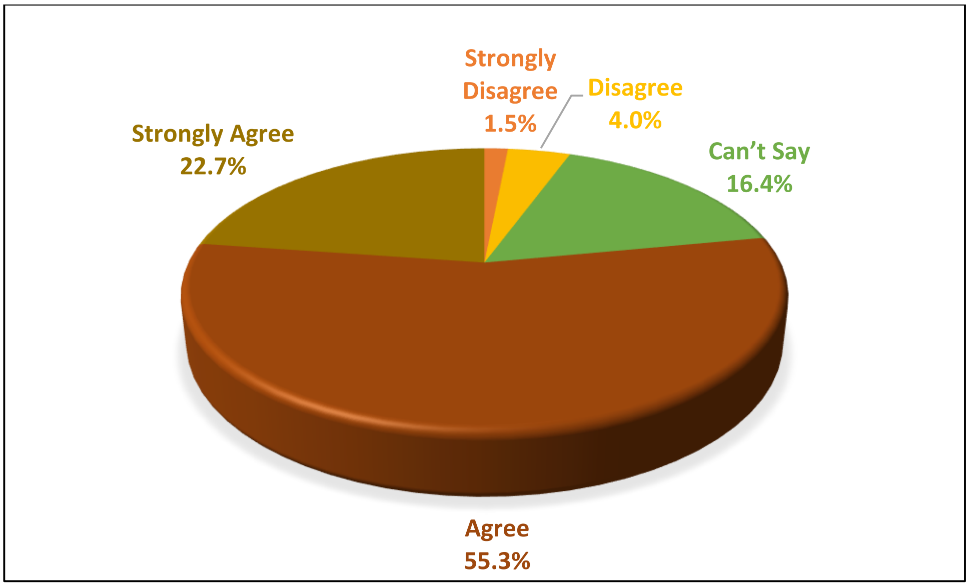
Results obtained follows the same pattern as of previous question no 14. Majority of smart home users (~75%) are ready to share their data to law enforcement/criminal investigating agency in case need. This means the smart home users can compromise on data sharing and privacy in times of need.

16. Do you think it's necessary to provide home visitors, a distinct role based management and operational authentication?

Role based device authentication and management is important in preventing unauthorized use of smart home device. When the usage is for home security it becomes very important to safeguard the entire smart home ecosystem from outsiders. Ignorance can lead to hazard. This question aims at understanding how smart home users allow access of their smart home devices to their home visitors.

Responses	Frequency	Percent
Strongly Disagree	6	1.5%
Disagree	16	4.0%
Can’t Say	65	16.4%
Agree	219	55.3%
Strongly Agree	90	22.7%
Total	396	100%

Table 4.16 Role based device authentication and management



Graph 4.16 Role based device authentication and management

Observations:

Responses revealed that 78% of smart home users have agreed that device access should be role based on, a very small 5.5% have shown their disagreement whereas 16.4% are not sure about role based device authentication and management.

Inference:

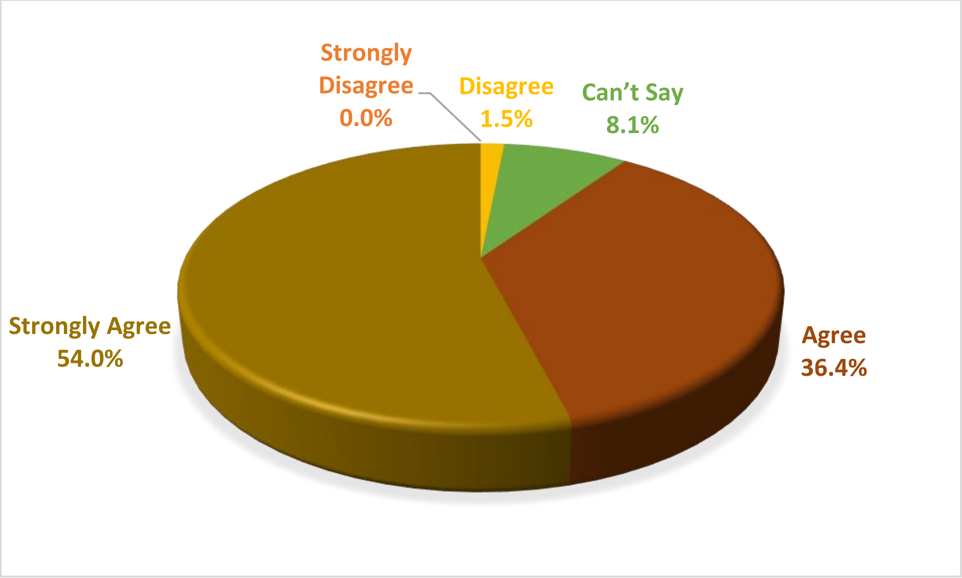
Majority of smart home users (78%) are aware of the ill consequences of allowing free device access to everyone. Whether the users are frequent home visitors or friends it is important to allow limited access of device to save your smart home ecosystem from security threats and data breach. 21.9% users are not aware or are ignorant about the fact.

17. Do you agree your Wi-Fi and Bluetooth should be set to a highest security level?

Hackers always target weak network and device. If Wi-Fi and Bluetooth based device operates at low level security they becomes vulnerable for such kinds of malicious attacks by the hackers. This question aims at collecting smart home user's response on the issue.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	6	1.5%
Can't Say	32	8.1%
Agree	144	36.4%
Strongly Agree	214	54%
Total	396	100%

Table 4.17 Security levels of Wi-Fi / Bluetooth



Graph 4.17 Security levels of Wi-Fi / Bluetooth

Observations:

Above table and graph depicts 54% respondents accepts the necessity of configuring the Wi-Fi with proper precautions. 36.4 % were having same opinion. 8.1% were natural about this. Very few 1.5% respondents were against this which is insignificant.

Inferences:

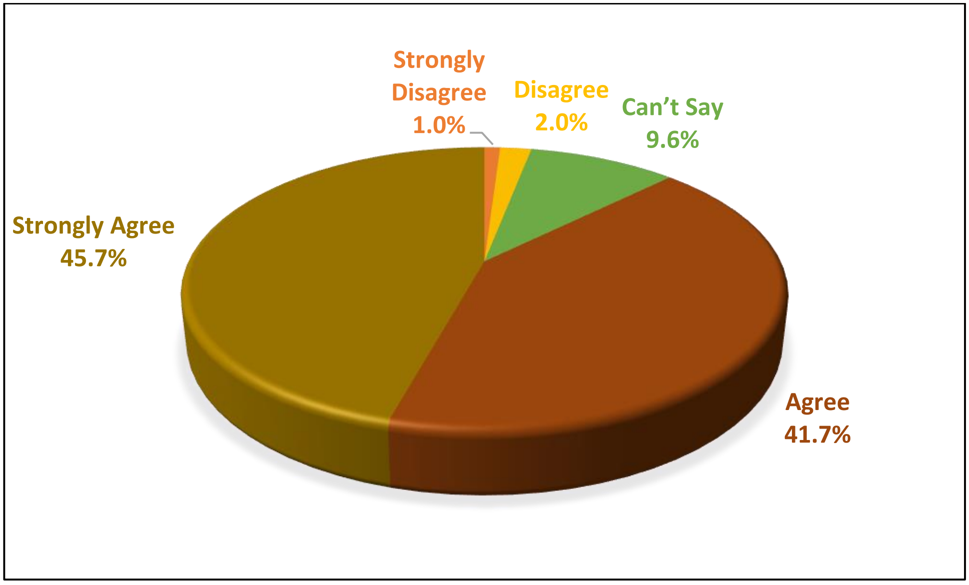
It is analysed 90.4% respondents knows the importance of configuring communicating devices for the sake of security.

18. Do you feel comfortable storing personal or family related information or videos on a smart home system?

In a smart home environment, users store personal and family related preferential data to get better service and feeling of smartness. The aim of this question is to understand smart home user's perception about storing such data on smart home ecosystem. This also helps in exploring whether people feel safe in storing their personal data/information over cloud. Due to the openness of IoT Environment trust and faith is a main concern.

Responses	Frequency	Percent
Strongly Disagree	4	1%
Disagree	8	2%
Can't Say	38	9.6%
Agree	165	41.7%
Strongly Agree	181	45.7%
Total	396	100%

Table 4.18 Storing of personal data on smart home system



Graph 4.18 storing of personal data on smart home system

Observations:

The responses received shows that 87.4% of the respondents prefer storing their personal/family related data whereas only 3% disagree of storing on smart home cloud. Only about 10% (~9.6%) were unsure.

Inferences:

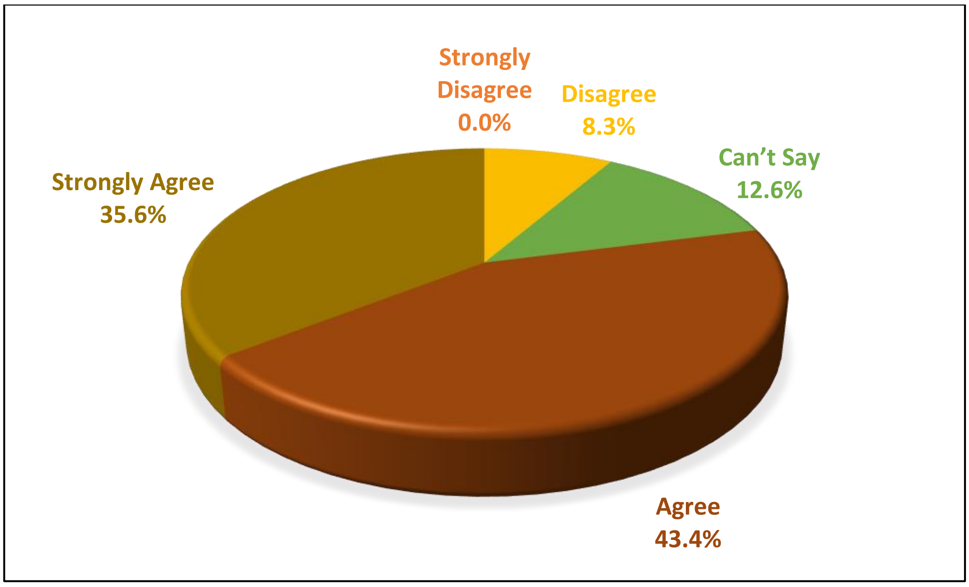
Majority of the respondents store their data over cloud. This may be due to the product requirement. But, it is important to know if the users are aware of the ill implication involved. As data breach happens frequently due to data compromise over cloud.

19. Do you agree that privacy is breached when one cannot regulate which information can be collected by smart devices (e.g., data stored by Alexa/Google Assistant)?

Privacy and security are the major challenges in smart home system. Home users prefer to have control on information collected by smart home devices. In a smart home environment, smart device voice assistant (i.e. Alexa) listens and collects all information for the user. But if compromised it can be a breach of user's privacy. The purpose of this question is to know users response on this issue.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	33	8.3%
Can't Say	50	12.6%
Agree	172	43.4%
Strongly Agree	141	35.6%
	396	**Total**

Table 4.19 Users control of information being shared



Graph 4.19 Users control of information being shared

Observations:

About 79% of the respondents have agreed that their privacy will be breached if they cannot regulate the data collected by smart home assistants. Very small 8.3% disagree, whereas only 12.6% are clueless.

Inferences:

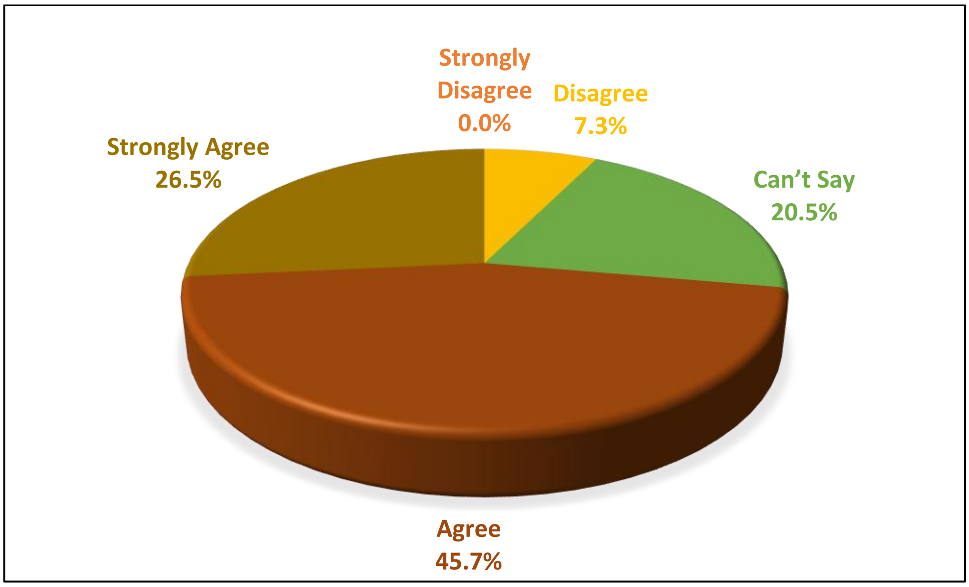
About 80% (~79) of the respondents know the severity of misuse of data collected by smart home assistant and data breach. Smart home privacy and security issue also depends on this response.

20. Do you think data stored in encrypted form will not be manipulated?

The best way to ensure confidentiality is to store data in encrypted form. The problem is of trust. This question tries to discovery the trust on technology and standard measures.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	29	7.3%
Can’t Say	81	20.5%
Agree	181	45.7%
Strongly Agree	105	26.5%
Total	396	100%

Table 4.20 Trust on technology



Graph 4.20 Trust on technology

Observations:

According to data collected from respondents 72.2% believes that if data is stored in encrypted form then data confidentiality can be maintained. Only 7.3% disagree whereas 20.5% were not sure about the effects of data encryption in smart home system.

Inferences:

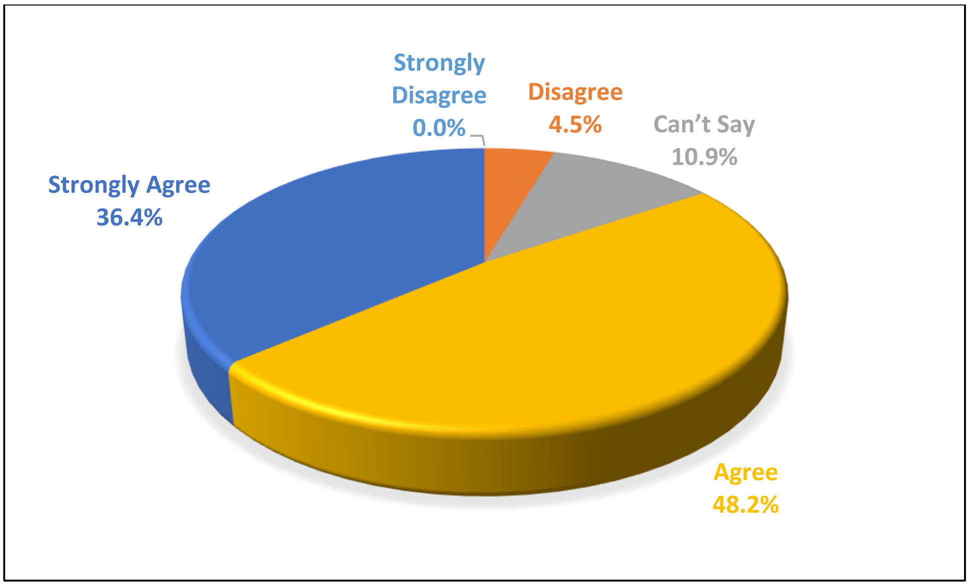
Majority of smart users are aware about importance of data encryption in ensuring data integrity. Those 20.5% respondents who are not sure about encryption needs to be given input on its relevance and importance.

21. Do you agree that "Device verification" is required to insure reliability of data source?

It is important to verify and validate the protection of IoT devices by using verification technique. This question aims at ensuring whether the user knows about device verification and its importance in ensuring reliability of data source.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	18	4.5%
Can't Say	43	10.9%
Agree	191	48.2%
Strongly Agree	144	36.4%
Total	396	100%

Table 4.21 Importance of device verification



Graph 4.21 Importance of device verification

Observations:

About 85%(~84.6%) of smart home users are aware about the importance of smart home device verification. A very small number i.e., 15% of respondents either disagree or have no idea regarding the importance of device verification.

Inferences:

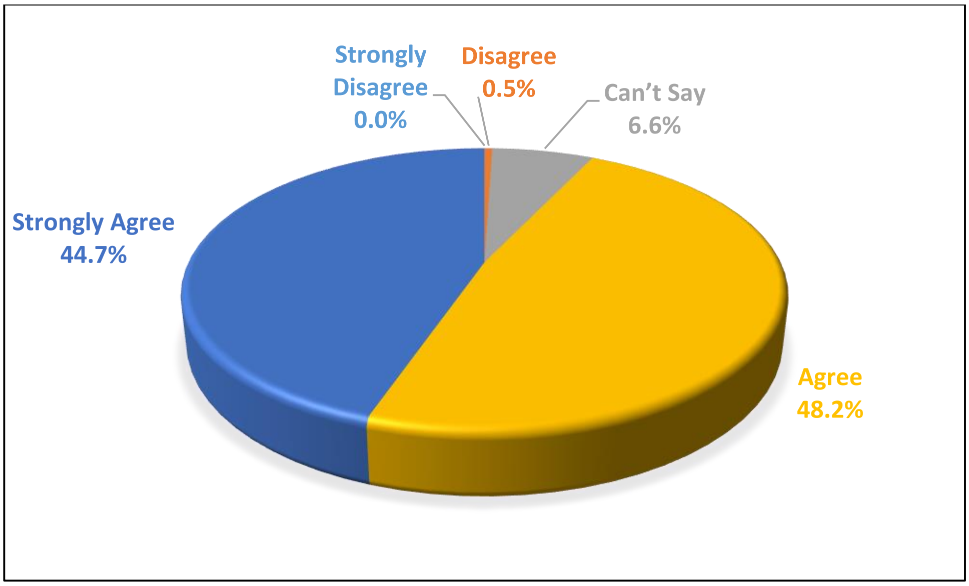
Respondents were pretty aware about the reliability of data source Majority of the respondents were in favour of “Device verification” feature in smart home ecosystem.

22. Do you believe that the loss of sensitive information might result in more serious consequences, such as a loss of reputation?

Loss, misuse, alteration or illegal access to private information can significantly impact the privacy. This question tries to find smart home users consciousness about personal information.

Responses	**Frequency**	**Percent**
Strongly Disagree	0	0
Disagree	2	0.5%
Can’t Say	26	6.5%
Agree	191	48.2%
Strongly Agree	177	44.7%
Total	396	100

Table 4.22 consequences of loss of sensitive information



Graph 4.22 consequences of loss of sensitive information

Observations:

About 93.4% of the respondents have shown their concern regarding loss of sensitive data. Only 6.1% have no idea as against 0.5% who feel loss of sensitive data is not important.

Inferences:

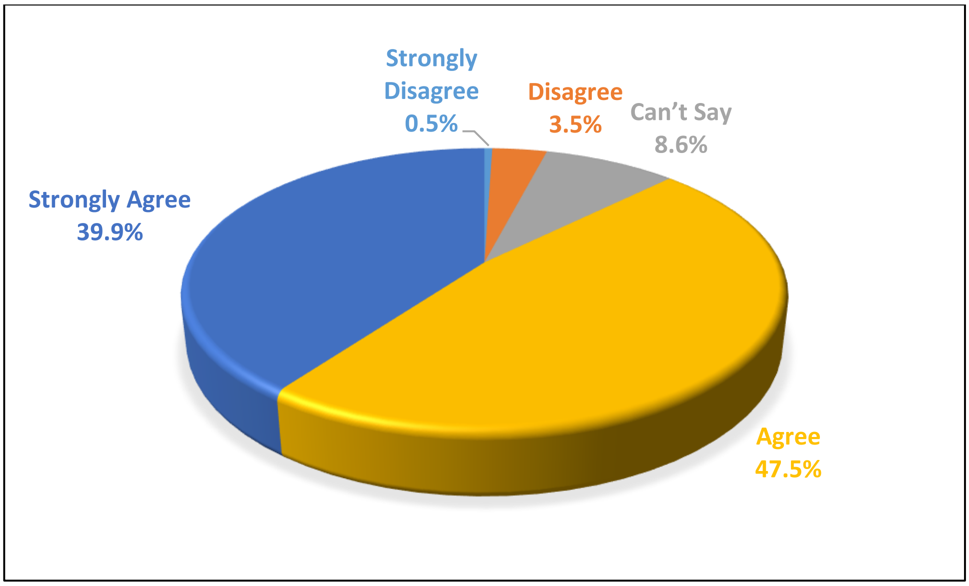
It is clear from the responses and the graph that majority of the respondents really care about the reputation loss due to loss of sensitive data.

23. Do you feel it is essential to place your devices in a safe (not easily reachable) location to prevent theft or damage?

Physical security of devices is equally important for seamless working of the system. It is necessary to place the smart home devices at secured place. This will prevent physical damage to the system and avert possible misuse of the data stored in the device.

Responses	Frequency	Percent
Strongly Disagree	2	0.5%
Disagree	14	3.5%
Can’t Say	34	8.6%
Agree	188	47.5%
Strongly Agree	158	39.9%
Total	396	100

Table 4.23 Physical Security of devices



Graph 4.23 Physical Security of devices

Observations:

87.4 % respondents agree the device must be kept at secure location inside the home. Only 4% disagree to this fact whereas 8.6% respondents were unsure about device security and its implication on smart home security and privacy.

Inferences:

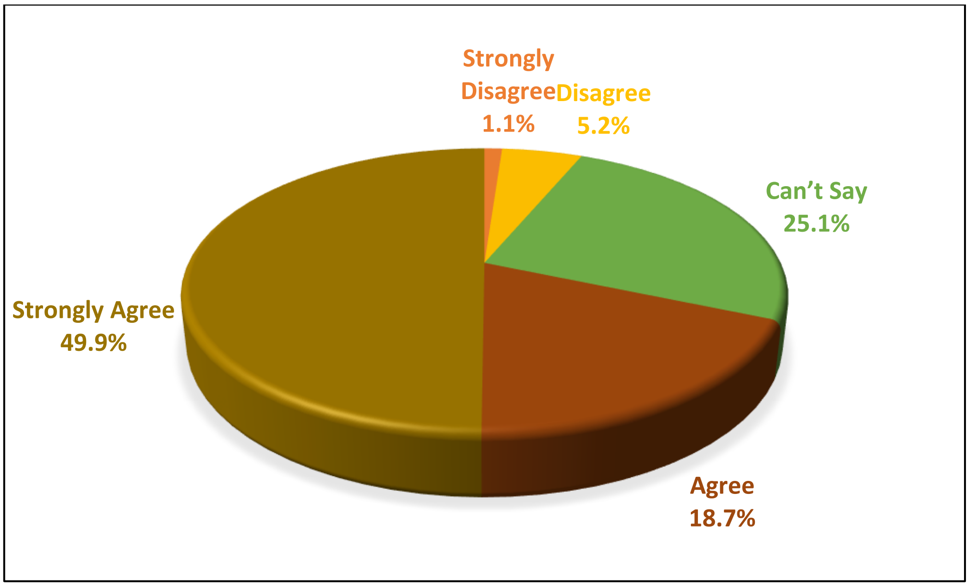
Reasonably amount of users are aware about keeping smart home device at a secured location. This could be because few of them may be knowing its importance. One possibility of high cost of these devices cannot be ignored. Few users have revealed during interview that they keep it at secured location due to its cost.

24. Do you feel worried about unresponsiveness of security devices?

Smart home devices/gadgets may become frozen of hanged. When they become unresponsive they will fail to give services. So trouble shooting mechanism should be opted. There could be reasons such as hackers attack too. The aim of this question is to understand smart home user's awareness on device unresponsiveness.

Responses	Frequency	Percent
Strongly Disagree	9	2.3%
Disagree	41	10.4%
Can't Say	198	40.0%
Agree	148	37.4%
Strongly Agree	394	99.5%
Total	396	100

Table 4.24 Unresponsiveness of security devices



Graph 4.24 Unresponsiveness of security devices

Observations:

It can be seen from the responses received that 87.3% of the respondents are concern about unresponsive devices, whereas only 12.7% do not realize the importance of their smart home devices becoming unresponsive. Device unresponsiveness can be a threat to the smart home security and this should be known to the smart home users.

Inferences:

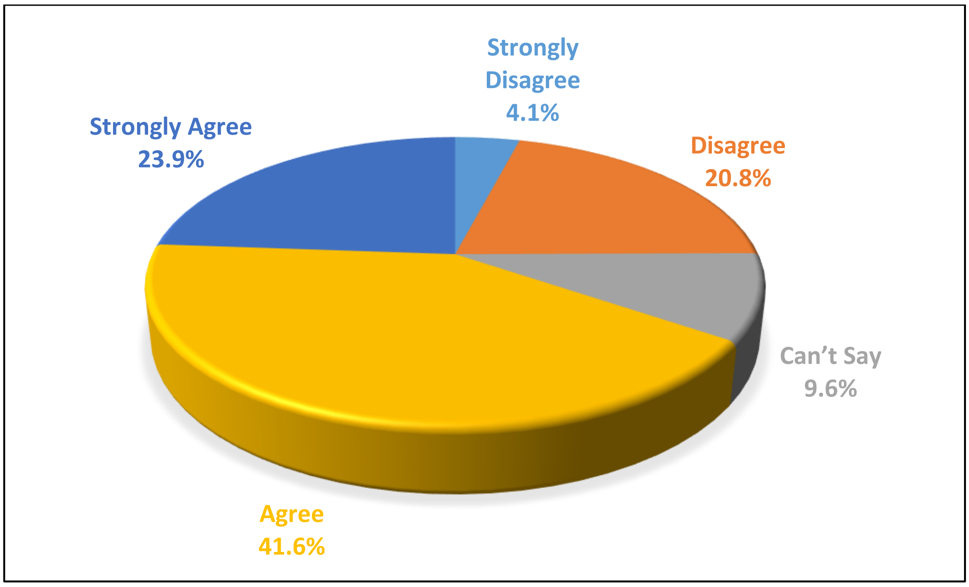
Result of the responses is a clear cut indication that smart home users are aware of the unresponsiveness, but, 12.7% users need to be educate on the security threats due to device unresponsiveness as the devices need to be constantly connected to the system to work properly.

25. Do you prefer ease of use over smart home security?

Safety and ease-of-use (convenience) are two important aspect of smart home security. It is important to compare these two factors. This question aims to find the users preference about usability and security.

Responses	Frequency	Percent
Strongly Disagree	16	4%
Disagree	82	20.7%
Can’t Say	38	9.6%
Agree	164	41.4%
Strongly Agree	94	23.7%
Total	394	99.5%

Table 4.25 Convenience and device security



Graph 4.25 Convenience and device security

Observations:

Around 65.5% respondents said they prefer ease of ease-of-use over security in contrast to 24.9% respondents have disagreed. 9.6% respondents were neutral.

Inferences:

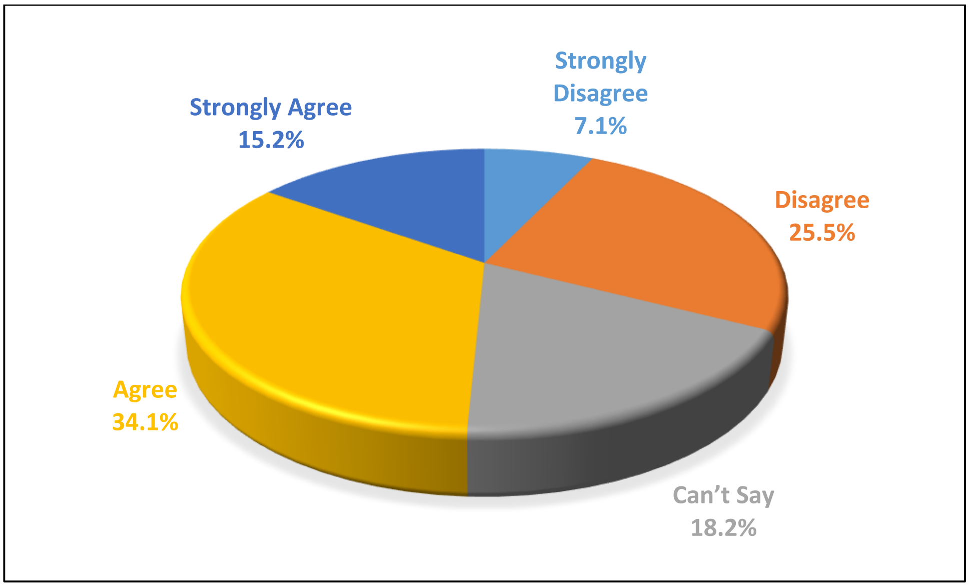
Security & safety would never be the top priority for most people relative to ease of use. Developer need to consider this point that people prefer continuance but security is also an important issue.

26. Do you think security measures reduce user-friendliness?

If the security system is not user friendly then users try to disable the security features that results into security breach. The aim of this question is to understand smart home user perception about user friendliness and device security.

Responses	Frequency	Percent
Strongly Disagree	28	7.1%
Disagree	101	25.5%
Can’t Say	72	18.2%
Agree	135	34.1%
Strongly Agree	60	15.2%
Total	396	100%

Table 4.26 Device security and user friendliness



Graph 4.26 Device security and user friendliness

Observations:

49.3% of the respondents feel that device security measures reduce the user friendliness. 32.6% respondents disagree to this whereas 18.2% respondents are unsure.

Inferences:

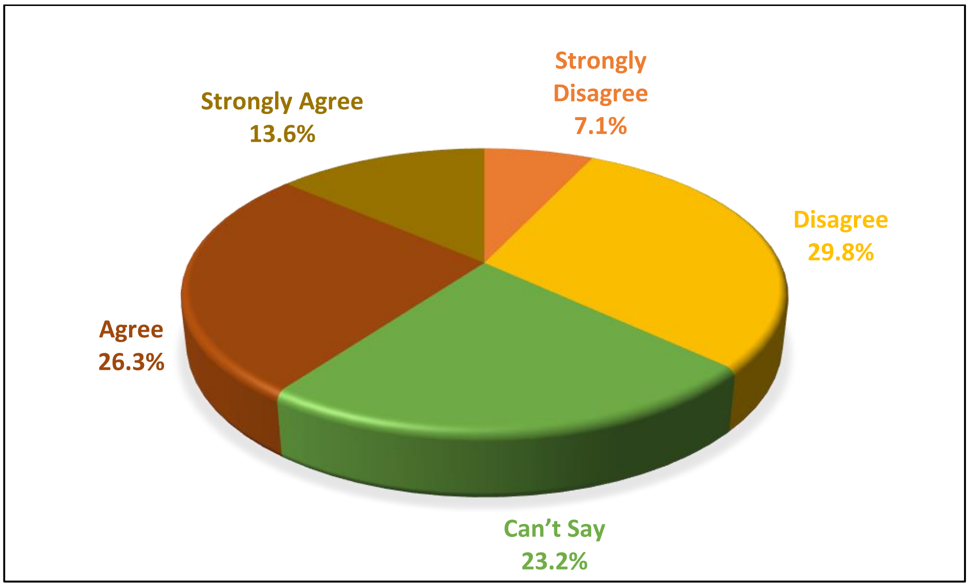
User friendliness is an important for optimal utilization of devices, therefore device manufacturer should provide easy devise access and management

27. Is it more important to consider the cost of smart device automation and related services over security concerns?

This question attempts to discover the importance of parameters like for a smart home user which is a prime consideration cost or security.

Responses	Frequency	Percent
Strongly Disagree	28	7.1%
Disagree	118	29.8%
Can’t Say	92	23.2%
Agree	104	26.3%
Strongly Agree	54	13.6%
Total	396	100%

Table 4.27 Relevance of cost and security in smart home



Graph 4.27 Relevance of cost and security in smart home

Observations:

Out of total 396 responses received, 39.9% respondents have agreed that cost of automation is important whereas 36.9% have given security more priority than the cost of automation. Surprisingly a greater amount of respondents 23.2% were not able to differentiate the trade-off between security and the cost of smart home automation.

Inferences:

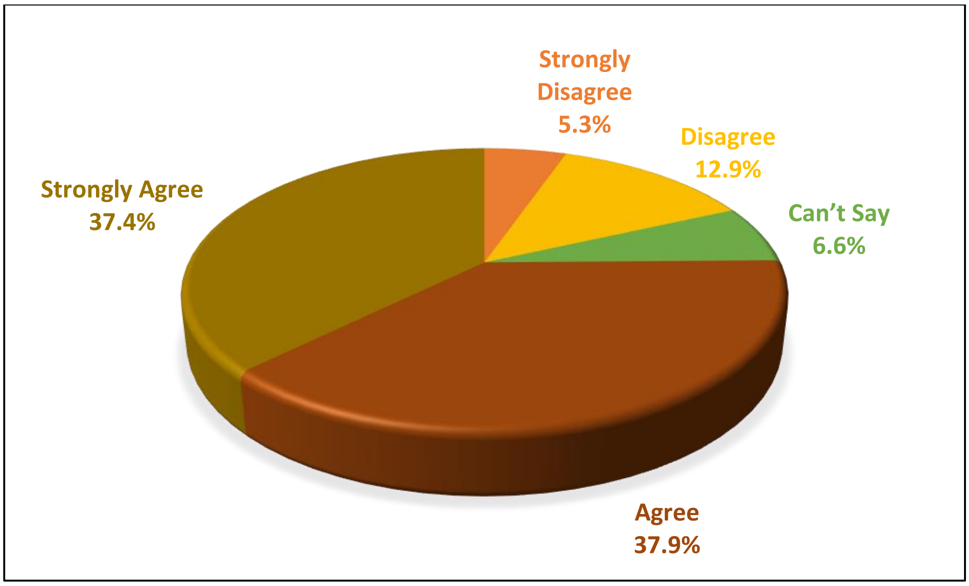
Respondents have given mixed responses to the question related to security and cost trade off. This means importance of security is still needs to be developed. Financial factors no doubt are important but if compromised, the losses will be insane.

28. Do you really feel that system access should be checked regularly? (Like password updates, security updates from manufacturer)

The ultimate aim of a user access analysis is to reduce the possibility of security violations by restricting access to sensitive data and resources. If not reviewed properly, user may be in danger.

Responses	Frequency	Percent
Strongly Disagree	21	5.3%
Disagree	51	12.9%
Can’t Say	26	6.6%
Agree	150	37.9%
Strongly Agree	148	37.4%
Total	396	100%

Table 4.28 Importance of security updates



Graph 4.28 Importance of security updates

Observations:

High percentage (75.3 %) of respondents agreed that the access to smart home security system should be reviewed from time to time by manufacturer or service provider. Only 18.2% were in appose to this statement and 6.6% were unaware.

Inferences:

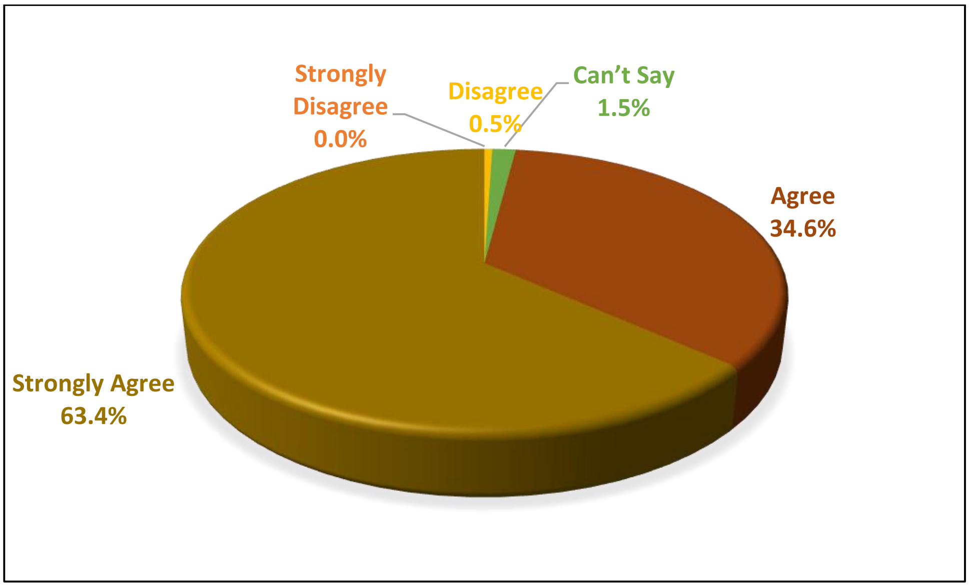
Every users may not be aware of managing the security updates and related activities. Therefore, majority of smart home users depends upon the services provided by the device manufacturer.

29. Do you think smart device malfunctions should be notified to the users on real time?

Notifications are a powerful tool for modern smart devices. With the intelligent system many dangers/ threats attempts can be easily managed. If undesirable access/attempt to access smart devices be brought to the knowledge of smart home users, such type of breaches can be curbed, the purpose of this question is to understand user's knowledge on this issue.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	2	0.5%
Can't Say	6	1.5%
Agree	137	34.6%
Strongly Agree	251	63.4%
Total	396	100%

Table 4.29 Real time alerts of device malfunction



Graph 4.29 Real time alerts of device malfunction

Observations:

Majority percentage of respondents 98% have agreed that they should be notified on real-time basis regarding any such incidents when their smart home device malfunctions. Only 0.5 % respondents have disagreed and 1.5% were having no idea on this aspect of system.

Inferences:

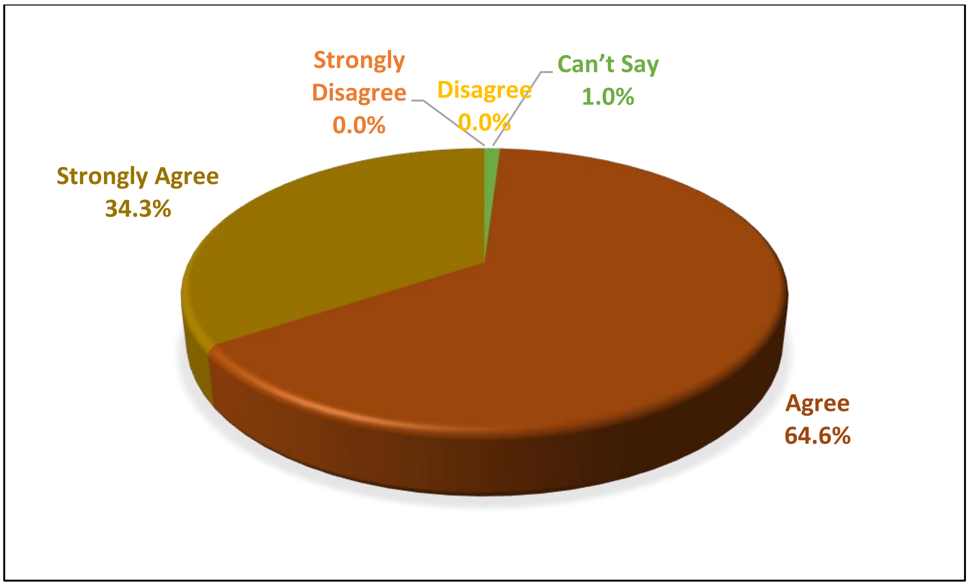
Large number of percentage of respondents wants to get real time notifications as it will keep home users informed and will help them in taking corrective actions.

30. Do you expect smart home system should send alert logs in case of data modification or alteration?

IOT devices collects massive amount of data. It is necessary to protect user's data which is very much sensitive and private. This can be possible only if smart home system sends the change log data to smart home users.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	0	0
Can't Say	4	1%
Agree	256	64.6%
Strongly Agree	136	34.3%
Total	396	100%

Table 4.30 Alerts on data alteration



Graph 4.30 Alerts on data alteration

Observations:

Barring only 1% users the remaining 99% wants data change alert logs to be shared.

Inferences:

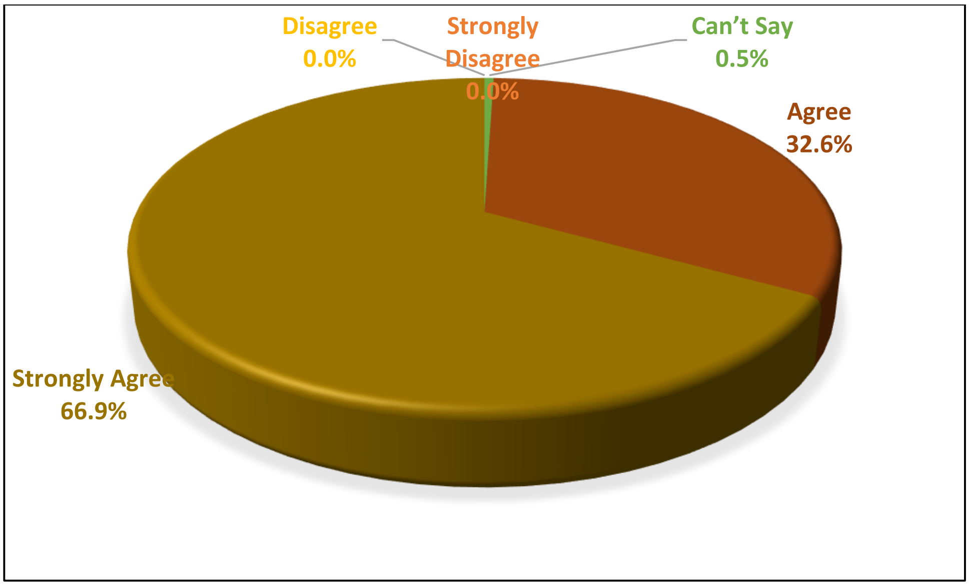
This confirms that privacy is given utmost importance by the smart home users.

31. Smart home users should be notified about abnormality related to smart home environment on real time basis.

Overall smart home environment control and monitoring is among the important features of an IoT based system. It is necessary to detect abnormities and send the real time alerts to the user.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	0	0
Can't Say	2	0.5%
Agree	129	32.6%
Strongly Agree	265	66.9%
Total	396	100%

Table 4.31 Real time notification for abnormalities in smart home system



Graph 4.31 Real time notification for abnormalities in smart home system

Observations:

Out of the total 396 respondents, 99.5% have agreed that they should be sent real-time alerts in case if any abnormality is detected in smart home environment. Only 0.5% of respondents are unsure about the importance of alert logs.

Inferences:

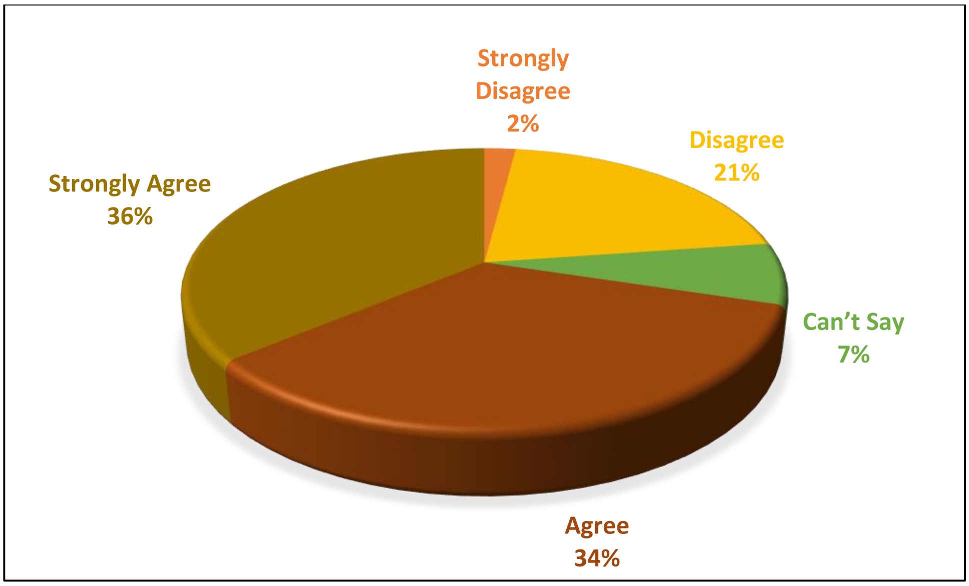
People always want to be informed about the abnormalities that happen so that they can take quick actions or arrived at certain solutions to the problems.

32. Do you feel comfortable in carrying online /financial transactions due to security purpose (e.g. hacking of Wi-Fi)?

E-banking or internet banking has become most convenient method of making payments over internet. It provides many advantages like speedy money transfer, efficiency etc. But it has threat of hacking. Many people hesitate to avail online financial transition facility.

Responses	Frequency	Percent
Strongly Disagree	8	2%
Disagree	82	20.7%
Can't Say	28	7.1%
Agree	135	34.1%
Strongly Agree	143	36.1%
Total	396	100%

Table 4.32 Comfortability in doing online transaction



Graph 4.32 Comfortability in doing online transaction

Observations:

About 70% of the respondents have said that they are comfortable in carrying online/financial transaction over Wi-Fi network and do not worry about any security threats. Only about 21% have shown fear due to security reasons whereas 7.1% respondents were unsure.

Inferences:

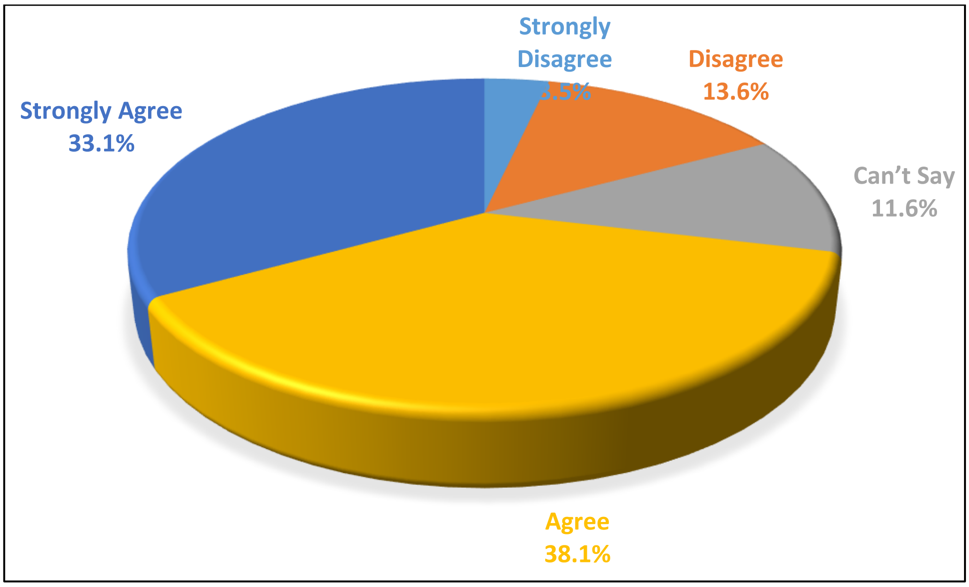
As many of us know the online frauds were growing day by day, people do care about the threats and its consequences. It is necessary that legal protection needs to be provided.

33. Do you prefer branded device over local manufactured?

Every users prefer to buy the devices that ultimately lowers the risk of being compromised. Branded products comes with responsibility and accountability. This question tries to find out the trust concern related to the smart home products.

Responses	Frequency	Percent
Strongly Disagree	14	3.5%
Disagree	54	13.6%
Can’t Say	46	11.6%
Agree	151	38.1%
Strongly Agree	131	33.1%
Total	396	100%

Table 4.33 Users preference of branded device over local



Graph 4.33 Users preference of branded device over local

Observations:

Approximately 71.2% respondents have given preference to the branded products. Still 15.1% were against this as cost may be the issue for them. 11.6% respondents were neutral.

Inferences:

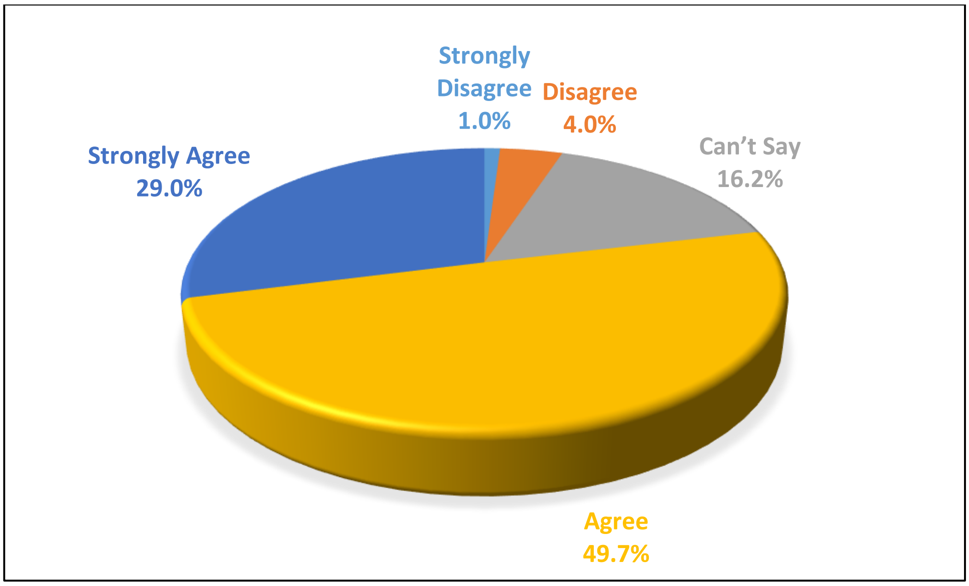
Larger percentage of respondents prefers to buy to branded products over local manufacturer. The reason could be trust on brands.

34. Do you believe that living in a smart home will safeguard your privacy and security?

Smart home devices provide convenience, wellness, energy efficiency, safety and automation. But the safety and security is the main challenges. This question tries to focus specifically on user's privacy and security.

Responses	Frequency	Percent
Strongly Disagree	4	1%
Disagree	16	4%
Can't Say	64	16.2%
Agree	197	49.7%
Strongly Agree	115	29%
Total	396	100%

Table 4.34 Do smart home safeguard privacy & security?



Graph 4.34 Do smart home safeguard privacy & security?

Observations:

About 79% of the respondents have agreed that they feel smart home safeguard their privacy and security. Only 5% disagree and 16% are unsure about this.

Inferences:

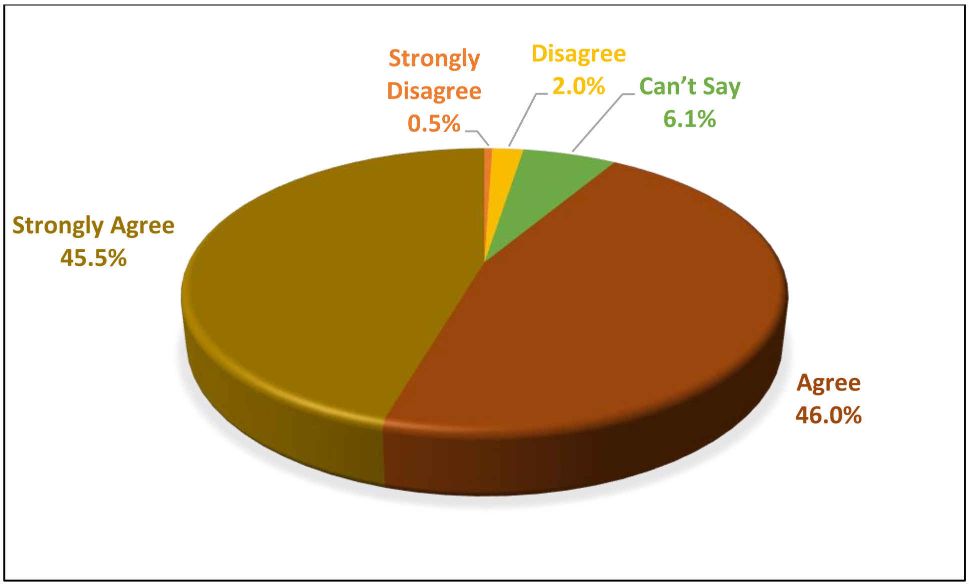
It can be interpreted from data that majority of respondents have are opted smart home with a view of protecting their personal data, security and privacy.

35. I believe it is essential that smart home devices should have built-in security features.

The aim of this question is to understand smart home user's perception regarding built-in security features. In order to have a secured home, device should be equipped with security features.

Responses	Frequency	Percent
Strongly Disagree	2	0.5%
Disagree	8	2%
Can't Say	24	6.1%
Agree	182	46%
Strongly Agree	180	45.5%
Total	396	100%

Table 4.35 Built-in security features in smart home devices



Graph 4.35 Built-in security features in smart home devices

Observations:

The above table shows that 45.5% respondents' desires that Companies which provides smart devices should be built in security features. Further 46% were also in favour of the same. Just 2.5% were against this. 6.1% were ignorant about having built-in security features.

Inferences:

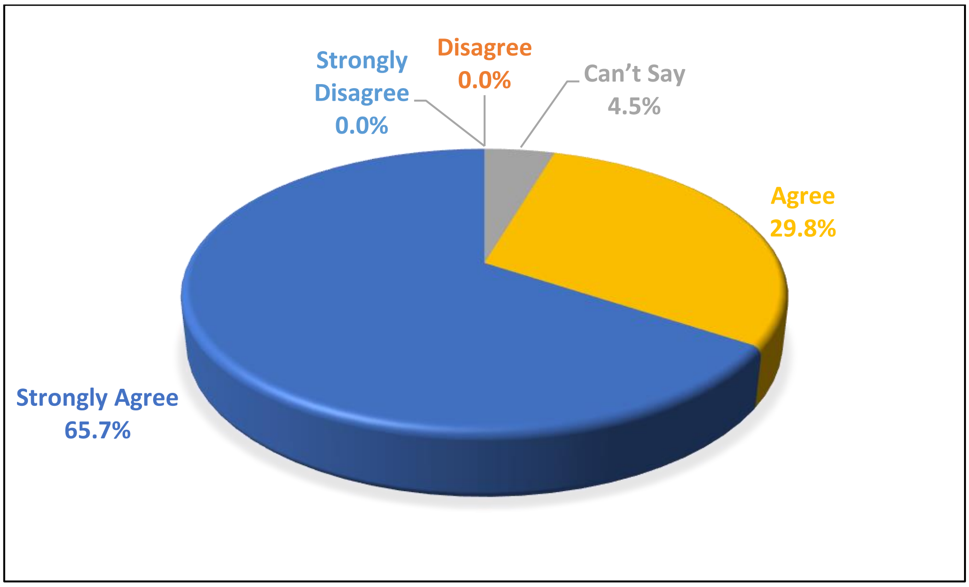
Approximately 90% of people are in the opinion that the companies who develop the devices should provide the integral security features.

36. Do you feel there should be strict laws to preserve individual privacy?

India is on the way to hitting towards Data-driven digital Revolution, Data theft has become a new buzz word. So it becomes urgent need of today's society to have strict laws of privacy and confidentiality

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	0	0
Can't Say	18	4.5%
Agree	118	29.8%
Strongly Agree	260	65.7%
Total	396	100%

Table 4.36 Do you feel there should be strict laws to preserve individual privacy?



Graph 4.36 Do you feel there should be strict laws to preserve individual privacy?

Observations:

95.5% indisputably supported this statement that shows real need of support from law to preserve individual's privacy. Only 4.5% were neutral about this construct.

Inferences:

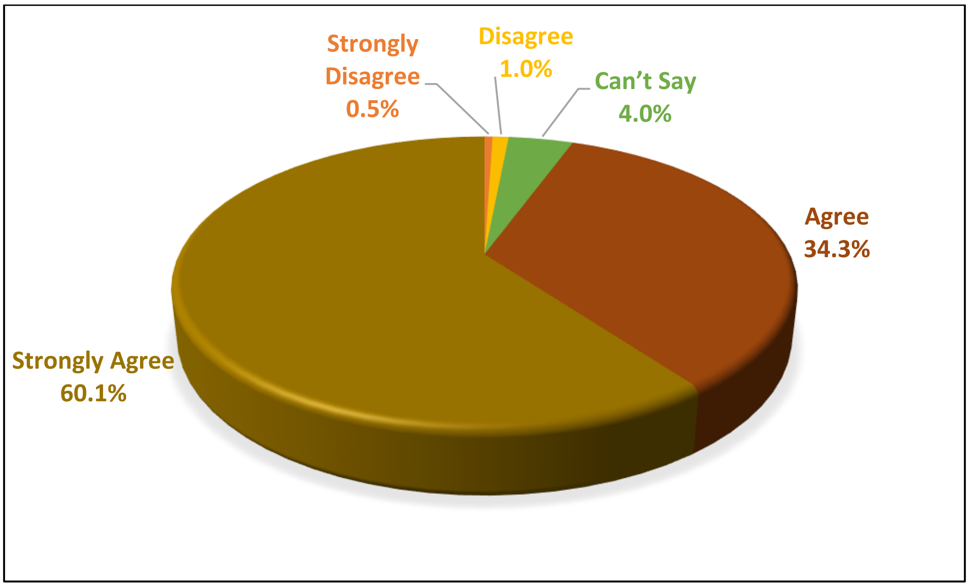
Privacy is a fundamental right of every individual. When personal data leaks, it may cause substantial harm to the reputation of an individual. It is therefore important that personal data privacy be preserved.

37. Do you think that the main concern for using smart home technology is home safety and security?

The home automation system is the pathway to the future, but it comes with its own collection of dangers and potential shortcomings. It is important to understand smart home users concern towards smart home technology. This question aims at understanding home safety and security issues.

Responses	Frequency	Percent
Strongly Disagree	2	0.5%
Disagree	4	1%
Can’t Say	16	4%
Agree	136	34.3%
Strongly Agree	238	60.1%
Total	396	100%

Table 4.37 Main concern of smart home technology



Graph 4.37 Main concern of smart home technology

Observations:

About 94.4% respondents feel that safety and security are the main reasons for implementing smart home environment. Only 1.5% of the respondents disagree to the reason whereas 4% are neutral.

Inferences:

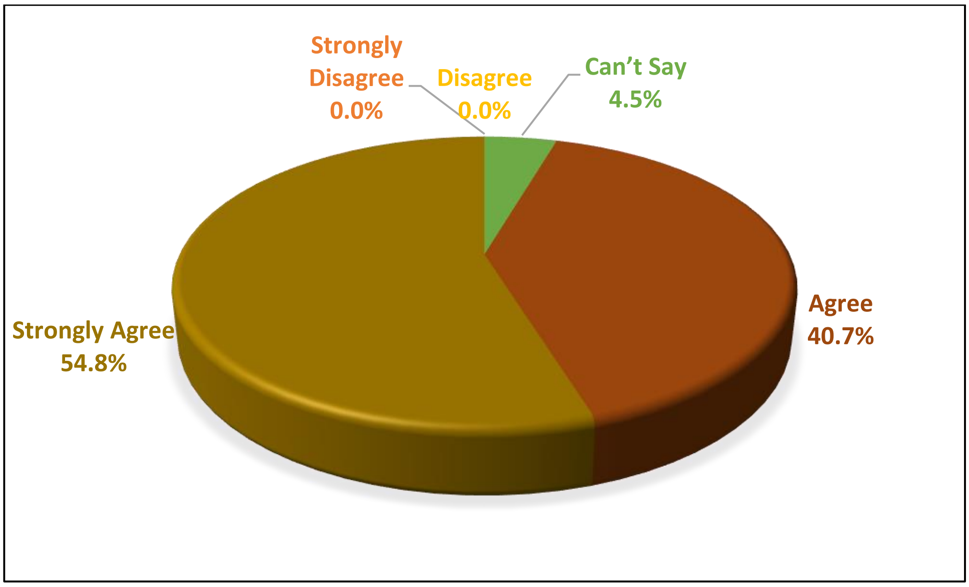
Security & safety is one of the main concerns of the smart home system. Theoretically, the idea of integrating smart home devices into your home sounds amazing. But when you know that every webcam, speaker, and information device is another potential entry point for hackers or cyber criminals, it's easy to understand why people are cautious.

38. Do you agree that losses suffered due to data leak might result in unimaginable consequences?

Stealing information is a criminal activity. The primary impact of cybercrime is financial cybercrime can involve several different forms of monitory criminal activity, including ransom-ware attacks, online scam, as well as attempts to hack financial account, payment card details. Cyber criminals can also exploit private information of the individual, as well as corporate data for theft and resale.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	0	0
Can't Say	18	4.5%
Agree	161	40.7%
Strongly Agree	217	54.8%
Total	396	100%

Table 4.38 Data leak might result in unimaginable consequences



Graph 4.38 Data leak might result in unimaginable consequences

Observations:

It seems people really concerns about data leaks and it consequences. Out of total responses received, 95.5% respondents were in favour of this threat. Just 4.5% were not ready to react on this issue.

Inferences:

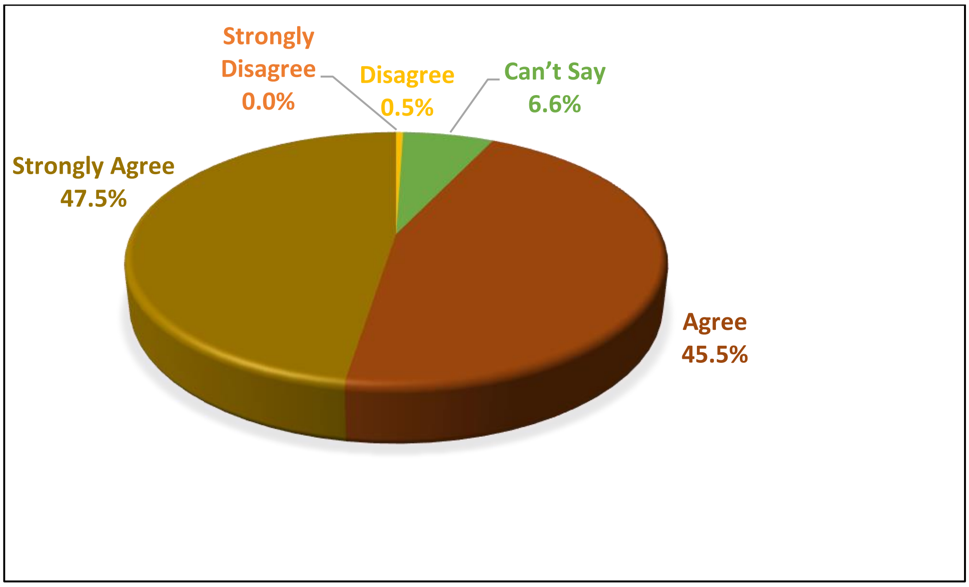
It is evident from above is smart home industry and its stakeholder need to take care of information leakages.

39. Do you consider identity that theft is the most serious threat to privacy? (for example, when misused in illegal purpose)

Identity theft is one of the most important issues facing countries across the globe. Identity theft concerns the illegal collection of personal details that determines one's identity for economic gain.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	2	0.5%
Can't Say	26	6.6%
Agree	180	45.5%
Strongly Agree	188	47.5%
Total	396	100%

Table 4.39 Is identity theft is serious threat?



Graph 4.39 Is identity theft is serious threat?

Observations:

The responses show that 92.2% respondents consider that identity theft is a greatest theft as against 0.5% respondents who disagree to this fact. 6.6% of the respondents were clueless about this.

Inferences:

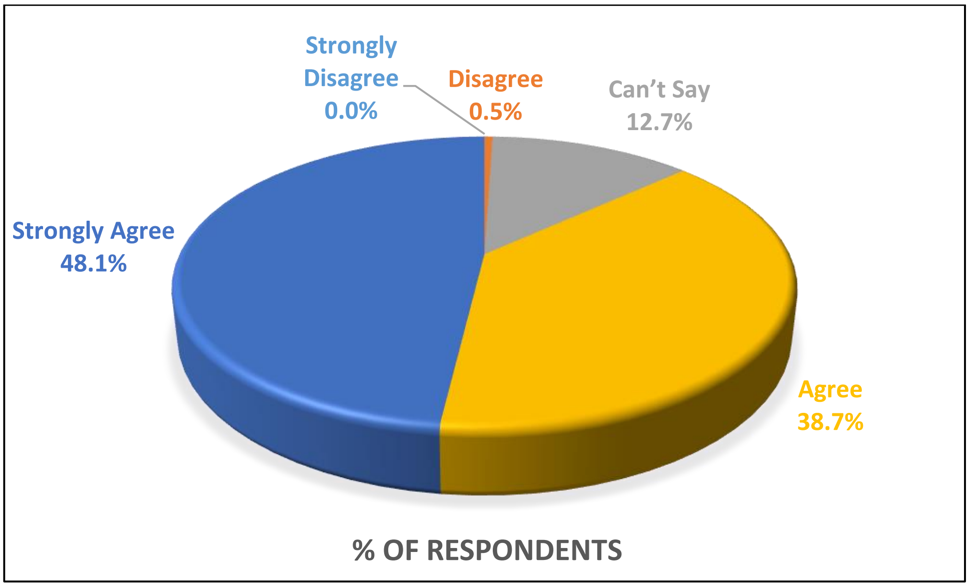
Identity theft is greatest risk, therefore it is necessary to protect the online identity by safeguarding the personal information like credit card number, bank details, and use only authentic sites for online transactions. Do not disclose password. In a smart home environment, data related to user’s identity may cause irreparable damage.

40. Do you believe that a breach of user privacy might result in financial losses?

This question tries to find the probable threats that arise due to privacy breaches. It may be possible that if hackers hack user's location then it may lead to robbery.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	2	0.5%
Can't Say	50	12.6%
Agree	152	38.4%
Strongly Agree	189	47.7%
Total	393	99.2%

Table 4.40 Financial losses due to privacy breach



Graph 4.40 Financial losses due to privacy breach

Observations:

Nearly 87% respondents feel that user's privacy breaches can lead to monetary losses, only 0.5% disagree that this could happen, whereas 12.6% respondents neither agree nor disagree to this.

Inferences:

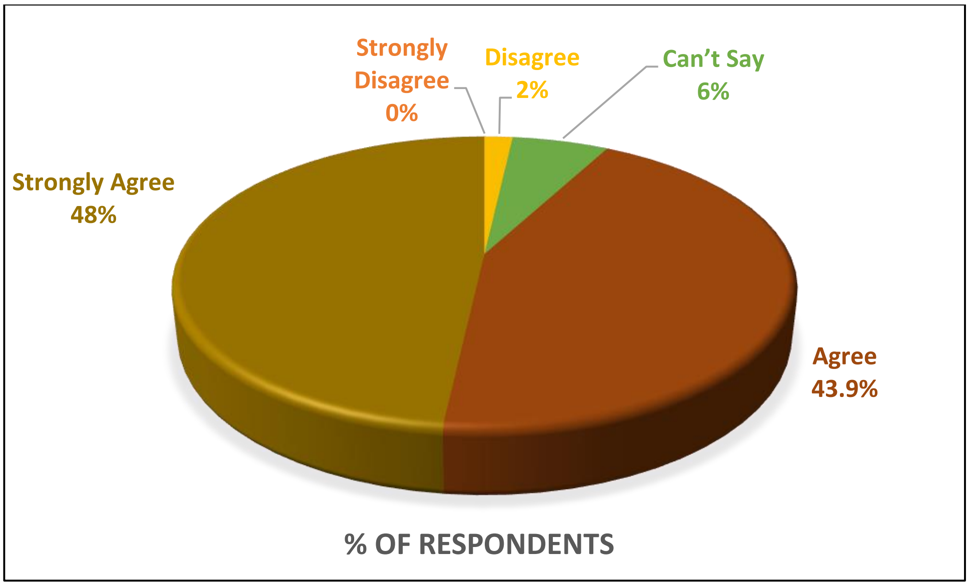
In particular, leakage of personal information by breach of data could lead to monetary losses. So care should be taken to protect the user privacy.

41. Do you think it is necessary to avoid using public Wi-Fi to access your smart home system remotely?

One can use smart home application to control home from a remote location. If same smart phone is operated using public Wi-Fi remotely then hacker can easily plant infected software (virus) in your smart home system

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	7	1.8%
Can't Say	24	6.1%
Agree	174	43.9%
Strongly Agree	191	48.2%
Total	396	100%

Table 4.41 Avoidance of public Wi-Fi access



Graph 4.41 Avoidance of public Wi-Fi access

Observations:

Around 92.2% respondents have agreed that public Wi-Fi are open and vulnerable to hackers. 6.1% respondents are unsure about security threats in an open Wi-Fi system whereas only 1.8% have disagreed.

Inferences:

Public Wi-Fi is available all over the place, from the local coffee shop to the restaurants and airports. Wi-Fi has made our lives a little easier, but it still presents a security risk to the sensitive details available on our laptops and smartphones. Do not connect personal bank accounts or confidential personal data on unsecured public networks. It is inferred that use of smart phone on the public Wi-Fi should be avoided as far as possible.

42. Do you agree that the most serious security risks to your smart home system are unauthorised access to the system, virus attacks, and denial of service?

Cybercrime cases are undoubtedly increasing every day. Unauthorised access, viruses, attacks were considered as a biggest challenges now a days.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	0	0
Can't Say	22	5.6%
Agree	167	42.2%
Strongly Agree	207	52.3%
Total	396	100%

Table 4.42 Virus attacks and DOS attacks are serious risk

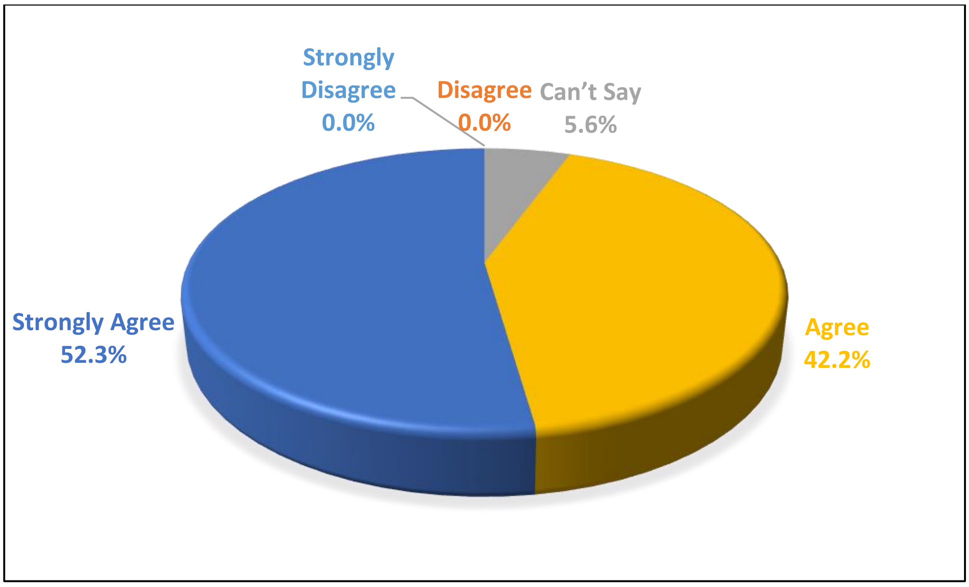


Table 4.42 Virus attacks and DOS attacks are serious risk

Observations:

Responses show that 94.4% of the respondents are aware of the threats arriving out of virus attacks, worms, DoS attacks and its consequences. Only 5.6% are unsure about these security threats on smart home ecosystem.

Inferences:

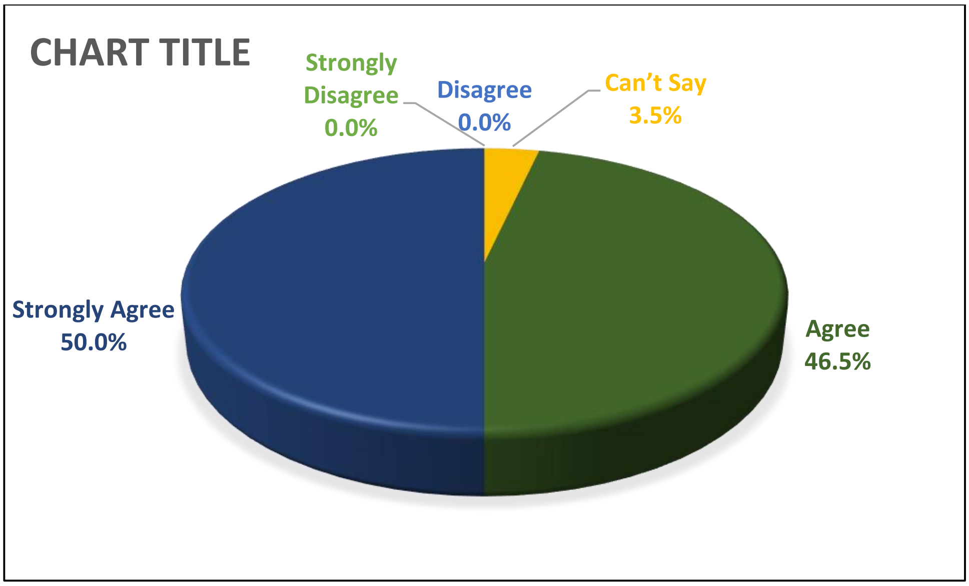
It is quite necessary that the smart home environment should be protected from different attacks. Few scenarios may be hacker gets access to your smart home air conditioner, gaining the opportunity to know when you may be out of the house. It can be an instance of DoS attack that force shut down of devices, may cause entire system to shut down or make them unavailable by disrupting internet connection.

43. Do you think raising security awareness for consumer is essential for protecting smart home system?

Smart home buyers may have some perceptions/queries about the products. So it is necessary to resolve it. The objective of this question is to explain the importance of "raising consumer awareness program" so that the consumer will buy right products.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	0	0
Can't Say	14	3.5%
Agree	184	46.5%
Strongly Agree	198	50%
Total	396	100%

Table 4.43 Relevance of consumer awareness for secure home system



Graph 4.43 Relevance of consumer awareness for secure home system

Observations:

Large percentages (96.5%) of respondents have agreed that raising the consumer awareness regarding the security is absolutely necessary. Only 3.5% were neutral but can be ignored.

Inferences:

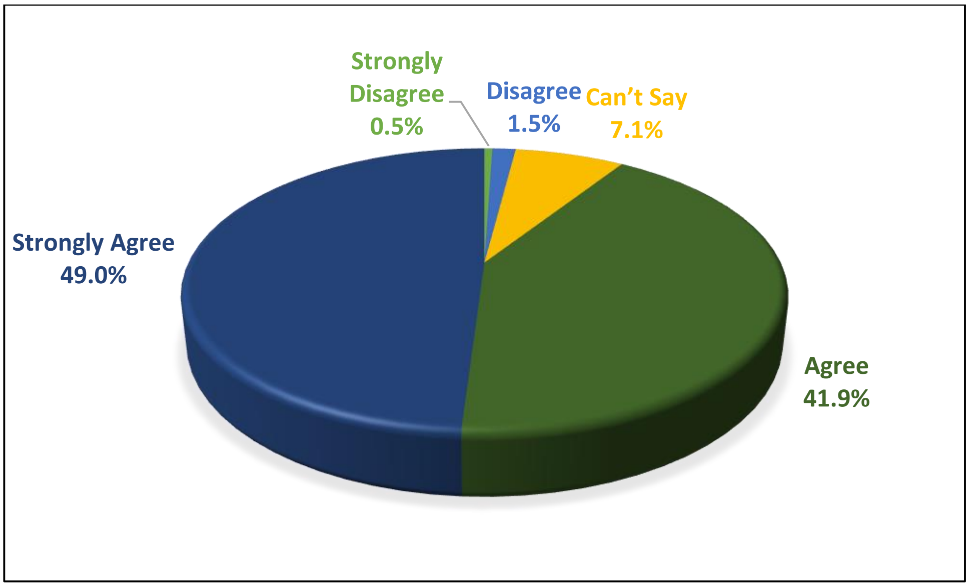
Respondents looks to be very thoughtful about the awareness program to avoid the potential risk and threats.

44. Do you feel careless or negligent end users are as dangerous as hackers?

Human related factor plays key role on security. Careless or negligent user may unknowingly exposed the data to the hackers. This can be considered as the most vulnerable thing to increase threat to the smart home Environment.

Responses	Frequency	Percent
Strongly Disagree	2	0.5%
Disagree	6	1.5%
Can't Say	28	7.1%
Agree	166	41.9%
Strongly Agree	194	49%
Total	396	100%

Table 4.44 Do you feel careless or negligent end users are as dangerous as hackers?



Graph 4.44 Do you feel careless or negligent end users are as dangerous as hackers?

Observations:

90.9% respondents have agreed that carelessness is a threat and it should be avoided as far as possible, only 2% of the respondents have disagreed to the fact. About 7% respondents are unsure about the consequences of the threats arriving out of user's negligence.

Inferences:

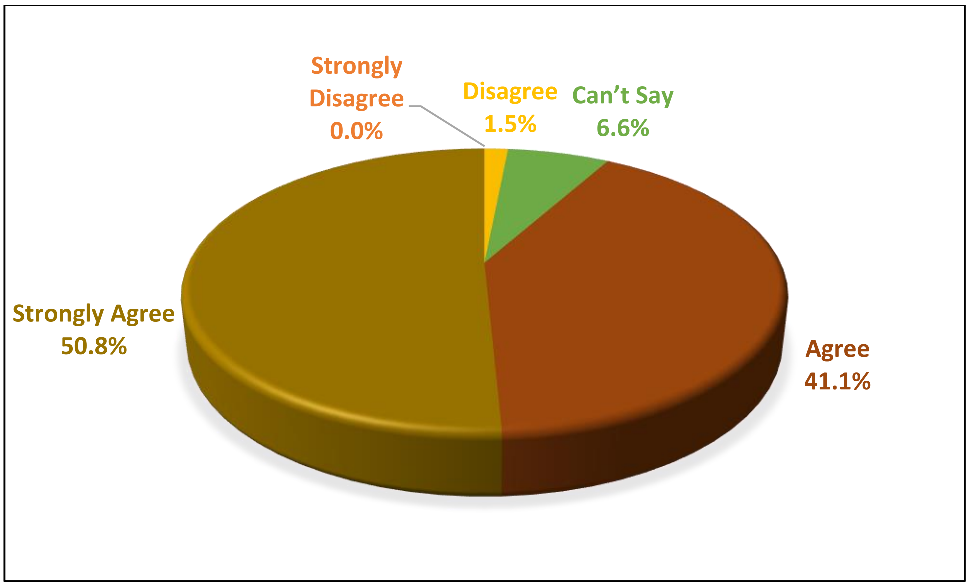
Carelessness, irresponsibility and lack of knowledge is greatest risk so must be avoided as far as possible.

45. Do you believe that users should be aware of the underlying technologies in order to protect themselves from data theft or hacking?

User need to have knowledge about how data theft happens, how to avoid it.

Responses	Frequency	Percent
Strongly Disagree	0	0
Disagree	6	1.5%
Can’t Say	26	6.6%
Agree	162	40.9%
Strongly Agree	200	50.5%
Total	394	99.5%

Table 4.45 Necessity of knowing technology to protect system from theft or hacking



Graph 4.45 Necessity of knowing technology to protect system from theft or hacking

Observations:

91.9% respondents have agreed that smart home users need to understand the technology being used in the devices and the best practices to avoid it. Only 1.5% of the respondents did not agreed to this whereas 6.6% were neutral on this aspect.

Inferences:

It can be analysed that user must be smart to user's smartness will add intelligence to smart home.

4.3. Hypothesis Testing

A research hypothesis (or scientific hypothesis) is an assumption of the expected relationship between variables or an interpretation of the occurrence, which is straightforward, precise, testable and verifiable. Hypothesis is framed by the researcher on the basis of knowledge acquired through literature review, existing models, frameworks, proven theories, etc. The hypothesis framed is then validated using appropriate statistical technique and statistic value.

In this research, author has framed three hypotheses. These hypotheses will address the objective set in the beginning of research.

H1: Smart home users are not fully aware about the data security features of smart home devices.

H2: Smart homes environment are significantly vulnerable to hackers if not configured Properly.

H3: Security awareness is directly related to an appropriate access control of smart home system.

The Hypothesis testing presented in this research involves following steps

1. Framing a null hypothesis
2. Framing of an alternative hypothesis against each null hypothesis
3. Setting up of the significance level (a) to test the hypothesised value
4. Calculate the test statistic and the corresponding p-value
5. Making inference from the test statistic.

4.3.1. Normality Test:

The data collected is checked for normal distribution so that appropriate statistical test can be applied. Parametric or non-parametric tests of statistics are applied to test the research hypothesis and this depends on the data distribution.

Descriptive statistics data was showing some skewness and in order to confirm the same author has conducted a normality test. In this research Shapiro-Wilk test of normality is used to understand data normality. The data normality is further verified using Kolmogorov-Smirnov (SN) test by comparing the score of the normal distributed test score with mean and deviations. Further, P-value decides whether data is normally distributed or not.

It has significance in terms of the selection of the parametric or non-parametric set of tests for hypothesis testing .If data is normal distributed then researcher makes use of parametric test and if it is non-normally distributed then non-parametric tests is used for testing the research hypothesis.

Null hypothesis for the test of normality is

H_0: Data not normally distributed.

H_a: Data is normally distributed.

Table 4.46 below present the normality test result.

Tests of Normality						
	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Statistic	**df**	**P Value**	**Statistic**	**df**	**P Value**
Gender	0.38	363	0	0.628	363	0
Edu_Qualification	0.268	363	0	0.816	363	0
Employment_Status	0.357	363	0	0.785	363	0
Monthly_income	0.257	363	0	0.784	363	0
How_long_Using_smart_home	0.243	363	0	0.798	363	0
Application_area_smart_home	0.284	363	0	0.824	363	0
Smart_Gadgets_U_Use	0.309	363	0	0.758	363	0
Data Authenticity in relation with authenticated devices	0.473	363	0	0.539	363	0
Sharing data with third party for advisement	0.401	363	0	0.574	363	0
Data sharing with relatives / care taker	0.253	363	0	0.877	363	0
Disabling security authentication in emergency condition	0.276	363	0	0.808	363	0
Allowing government agencies to use information generated by home	0.217	363	0	0.904	363	0
Allowing government agencies to give access in case of casualties (Fire brigade)	0.371	363	0	0.68	363	0
Allowing Law enforcement agencies to access data for crime investigation	0.327	363	0	0.814	363	0
Need to offer role based system for guest	0.307	363	0	0.815	363	0
Configuring Wi-Fi / Bluetooth high level of security	0.344	363	0	0.724	363	0
feeling safe storing personal / family confidential	0.276	363	0	0.757	363	0

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	P Value	Statistic	df	P Value
information on smart home system						
Possibility of Privacy violation when one can't control how much information is collected by smart devices (e.g. Google assistant)	0.258	363	0	0.819	363	0
Trust on Data stored in Encrypted form	0.252	363	0	0.854	363	0
Device verification to ensure Reliability of data source	0.259	363	0	0.794	363	0
Reputational loss due to leakage of sensitive information	0.296	363	0	0.743	363	0
Necessity to keep Devices at secure place	0.261	363	0	0.778	363	0
Unresponsive Security devices	0.247	363	0	0.792	363	0
Is ease-of- use preferred over security considerations?	0.287	363	0	0.852	363	0
Does Security measures reduces user-friendliness	0.233	363	0	0.894	363	0
Is cost of automation more important than security considerations	0.196	363	0	0.903	363	0
Necessity of system security updates reviewed from time to time (from manufacturer)	0.301	363	0	0.796	363	0
Getting real-time notification in case of device mal-function?	0.387	363	0	0.658	363	0
System should send alerts in case of data modification / alteration	0.418	363	0	0.627	363	0
User should get a real-time warning if an anomaly in the home environment is detected	0.432	363	0	0.603	363	0
Trust on doing online /financial transactions due to security purpose (e.g. hacking of Wi-Fi)	0.272	363	0	0.816	363	0
Prefer branded manufactured products over local manufacturers	0.278	363	0	0.833	363	0
Smart Home should provide privacy and Security	0.276	363	0	0.828	363	0
Necessity of having built in	0.279	363	0	0.737	363	0

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	P Value	Statistic	df	P Value
security features essential for companies which develop Smart devices should have						
Need to have strict laws to protect Individual Privacy	0.41	363	0	0.65	363	0
Home safety & security is main concern for implementation of Smart home Technology	0.361	363	0	0.676	363	0
Information leak can lead to unthinkable damages	0.348	363	0	0.712	363	0
Identity theft is the greatest risk against privacy for criminal activities	0.3	363	0	0.747	363	0
Violation of user privacy may result into financial losses.	0.302	363	0	0.772	363	0
I feel it is necessary to avoid public Wi-Fi for remote access to home system	0.289	363	0	0.753	363	0
Hackers Unauthorized access to System, are most critical security threats to your Smart home system	0.334	363	0	0.721	363	0
Raising security awareness consumer awareness is essential for protecting smart home system	0.323	363	0	0.716	363	0
I strongly feel Careless or negligent end users are as dangerous as hackers	0.292	363	0	0.744	363	0
Understand the underlying technology to protect from potential hacking / data theft is must	0.314	363	0	0.743	363	0
Extra	0.293	363	0	0.753	363	0

Table No 4.46 Test of Normality

In the table above, the P-value of Shapiro-Wilk and Kologorov-Smirnov test is 0.0. All the P–value is less than 0.05 (the level of significance), it is indicative to the fact that null hypothesis H_0 is accepted. The data is therefore showing non-normal distribution.

Considering the non-normality nature of data, non-parametric statistical test/s is used for hypothesis testing.

Hypothesis 1:

The first hypothesis is formulated to understand the smart home users' awareness about data security of the devices which are used in smart home ecosystem.

Null Hypothesis

H$_o$: Smart home users are not fully aware about the data security features of smart home devices.

Alternate hypothesis

H$_a$: Smart home users are fully aware about the data security features of smart home devices.

4.3.2. One sample KS Test

The awareness of the data security features of the smart home devices have been studied through 11 factors given in Table 4.47 below. In the survey questionnaire, respondents were asked to rate 11 factors related to data security of smart home devices (see Annexure A for detail).

Considering status of the hypothesis if the proposition value crosses 50%, it is considered adequate for the awareness. This could be tested using 'Binomial test, but binomial test is applicable on the responses of dichotomous type. Therefore, considering the scale and nature of the responses the second largest sample test i.e. KS test is used.

Statistic test Used for Hypothesis Testing:

One Sample KS test at 5% level of significance .i.e. α = .005

Variables		AU4	AR4	AR5	CO1	IN2	AV3	EU1	TR3	HF1	HF6	HF9
N		396	396	396	396	396	394	394	396	396	396	394
Normal Parameters[a]	Mean	1.9268	2.0631	1.5707	1.7096	1.8359	1.7741	2.3959	1.9823	1.4747	1.5328	1.5888
	Std. Deviation	0.86986	0.82894	0.70625	0.80127	0.7929	0.72206	1.17462	0.84025	0.6727	0.60079	0.68311
Most Extreme Differences	Absolute	0.275	0.311	0.331	0.269	0.264	0.25	0.287	0.279	0.361	0.335	0.313
	Positive	0.275	0.311	0.331	0.269	0.264	0.25	0.287	0.279	0.361	0.335	0.313

	Negative	-0.193	-0.242	-0.21	-0.188	-0.218	-0.247	-0.163	-0.218	-0.24	-0.259	-0.219
Kolmogorov-Smirnov Z		5.463	6.182	6.584	5.356	5.253	4.968	5.693	5.562	7.18	6.67	6.218
Asymp. Sig. (P Value)		0	0	0	0	0	0	0	0	0	0	0

Table 4.47 Test Result of One Sample KS Test

4.3.3. Description of the variables involved in KS test

Variables	Question from Questionnaire	Relevance / grouping
AU4	**Q14**	Disabling security under emergency
AR4	**Q18**	Authentication with role based actions
AR5	**Q19**	Security of connecting networks
CO1	**Q20**	Security of storage of personal confidential information
IN2	**Q23**	Verified device as reliable data source
AV3	**Q26**	Security risk of non-responsive devices
EU1	**Q27**	Preference to ease-of-use against security
TR3	**Q36**	Ensuring privacy & security in smart home
HF1	**Q39**	Importance of safety & security in smart home implementation
HF6	**Q44**	Unauthorized access as critical risk
HF9	**Q47**	User awareness regarding used technology & risk of theft

Table 4.48 Description of the Variables involved in KS Test

On the basis of the test statistic result, it is observed that all the P–values (with reference to table test result of 1-sample KS test) are less .005. Therefore null hypothesis is accepted and alternate hypothesis is rejected.

$$\left.\begin{array}{l}\mathbf{H_o: Accepted}\\ \mathbf{H_a: Rejected}\end{array}\right\} \quad \mathbf{P\text{-}value < .005}$$

Statistic test result of KS-test has revealed that the smart home users are not fully aware about the data security features of the smart home devices. It is therefore required that for better security smart home users be made aware on the security aspects of smart home devices.

Hypothesis No.2:

The first hypothesis is formulated to understand the users' perception regarding possible vulnerabilities in the smart home devices if they are not configured properly. Due to excessive use of IT/ITES related tools, the users have become too much dependent on using computer based systems. Considering the fact, all the smart home users are expected to know the vulnerabilities associated to improper configuration of their devices used in the ecosystem. Hypothesis 2 will address this aspect of the research.

Null Hypothesis

H_o: Smart homes environment are not significantly vulnerable to hackers, if not Configured properly

Alternate hypothesis

H_a: Smart homes environment are vulnerable to hackers, if not configured properly

To test this hypothesis, respondents were asked to rate the 11 factors related to the smart home environment vulnerability related issue and they were asked to rate these 11 factors on a 5-point Likert scale. The description of variables used in the test is given in table 4.49 below. In order to test the hypothesis and the significance level of its impact, non-parametric chi-square test is used. The identified 11 factors have been tested at 5% significance level.

Statistic test used for hypothesis testing:

Non Parametric Chi Square Test of Significant at 5% level of significance (i.e. α = .005)

4.3.4. Result of non-parametric Chi-Square test

Test Statistics											
Variables	**CO2**	**IN1**	**AV1**	**AV2**	**EU2**	**EU3**	**TR1**	**HF2**	**HF3**	**HF4**	**HF5**
Chi-Square	139.899[a]	121.051[a]	300.315[b]	382.586[c]	83.722[c]	69.960[c]	187.914[c]	159.561[d]	295.152[a]	231.214[e]	284.626[a]
df	3.000	3.000	3.000	4.000	4.000	4.000	4.000	2.000	3.000	3.000	3.000
P-Value	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Table 4.49 Chi-Square test of Significance

Description of variables in chi-square test

Variables	Questions from the Questionnaire	Relevance / grouping
CO2	**Q21**	Threat to privacy in case of loss of control
IN1	**Q22**	Reliability of data encryption
AV1	**Q24**	Damage due to loss of sensitive or confidential information
AV2	**Q25**	Physical security of devices
EU2	**Q28**	Impact of Security configuration on ease-of-use
EU3	**Q29**	Balance between cost of implementation and security requirements
TR1	**Q34**	Security Comfort while performing online transections
HF2	**Q40**	Impact of loss of confidential information
HF3	**Q41**	Impact of identity theft
HF4	**Q42**	Impact of losing privacy on financial cost
HF5	**Q43**	Reliability of public Wi-Fi

Table 4.50 Description of the Variables involved in Chi-square Test

The non-parametric Chi-square test applied on the 11 identified factors reveals that their P-value is less than .005 (at level of significance 5%), see table 4.48 above.

On the basis of the test statistic result, it is observed that all the P–values (with reference to Chi-square test) are less .005. Therefore null hypothesis is rejected and alternate hypothesis is accepted.

$$\left.\begin{array}{l}\textbf{H}_\textbf{o}\textbf{: Rejected}\\ \textbf{H}_\textbf{a}\textbf{: Accepted}\end{array}\right\}\quad \textbf{Chi-square test (P-value < .005)}$$

Statistic test result of Chi-square test shows that the devices in smart home environments are vulnerable to hackers if not configured properly. Existing vulnerabilities, poor configuration, default password are factors, can aid hacker in compromising devices.

Hypothesis No.3

The third hypothesis is formulated to understand whether the security awareness of smart home users has anything to do with the way they access their smart home environment and the devices in that ecosystem. The idea is to identify whether there is any correlation between the security awareness of smart home users and access control mechanism they follow to secure the smart home ecosystem and the devices. It is important to understand whether the users are able to manage the smart home environment and the devices in the ecosystem after knowing the importance of data security in smart home system.

Null Hypothesis

H_o: The security awareness is not directly related to the access controls of smart home system and devices

Alternate hypothesis

H_a: The security awareness is directly related to the access controls of smart home system and devices

4.3.5. Correlation test for security awareness and access control in smart home

To test the third hypothesis, spearman's correlation coefficient is used. Factors relating to the security awareness among smart home users and the access control mechanism used in smart home environment are tested using Spearman Rho (r_s) rank correlation coefficient.

Correlation coefficient is the best way to examine the strength of association between two variables. Two most popular correlation tests are Pearson and Spearman, out of the two Pearson is suggested on normally distributed variables whereas Spearman is suggested on nor-normal distributed variables.

The condition cited in one of the journal (Schober and Boer et al 2018) states that Spearman rank correlation is useful when the variable is on ordinal scale and non-normally distributed. Other condition for using Spearman rank correlation is that the two variables must be monotonically related as it tests the strength and direction of the monotonic association between two variables.

To test the third hypothesis, two groups are created so that relationship among security awareness and access control is analysed as below:

1. First group comprises of four variables from the survey questionnaire which were related to users' awareness on smart home security (Q11, Q12, Q13 and Q46).
2. Second group comprises four variable from the survey questionnaire which were related to smart home access control method (Q15, Q16, Q17 and Q18)

Refer to table 4.52 below for more detail.

Author has studied the scatter plot to study the relationship of the variables from the above group, out of total 16 graphs, only 4 are showing non-monotonic relationship otherwise 12 graphs shows proper monotonic relationship among awareness on security and smart home access control.

The association between the variables is predicted using Spearman rank correlation tests (r_s).

Interpretation of result is based on the proposed value published in a Turkish Journal (Akoglu, 2018). Author has made the Spearman correlation coefficient values interpretation using combination of coefficient values suggested by Dancey & Reidy, Quinnipac University and Chan YH in the areas of psychology, politics and medicine respectively.

Result is interpreted on the basis of table 4.51 below.

Correlation Coefficient	**Dancey & Reidy (Psychology)**	**Quinnipiac University (Politics)**	**Chan YH (Medicine)**
+1.0 to −1.0	Perfect	Perfect	Perfect
+0.9 to −0.9	Strong Very	Strong Very	Strong
+0.8 to −0.8	Strong	Very Strong	Very Strong
+0.7 to -0.7	Strong	Very Strong	Moderate
+0.6 to -0.6	Moderate	Strong	Moderate
+0.5 to -0.5	Moderate	Strong	Fair
+0.4 to -0.4	Moderate	Strong	Fair
+0.3 to -0.3	Weak	Moderate	Fair
+0.2 to -0.2	Weak	Weak	Poor
+0.1 to -0.1	Weak	Negligible	Poor
0.0	Zero	None	None

Table 4.51: Interpretation of Spearman's correlation coefficient

Spearman's Correlation Co-efficient						
			AR1	AR2	AR3	AR4
Spearman's rho	AU1	Correlation Coefficient	.018	.184	.021	.039
		Sig. (2-tailed)	.715	.000	.671	.443
		Interpretation	Very Weak	Very Weak	Very Weak	Very Weak
	AU2	Correlation Coefficient	.049	.251	.105	.060
		Sig. (2-tailed)	.334	.000	.037	.232
		Interpretation	Very Weak	Weak	Very Weak	Very Weak
	AU3	Correlation Coefficient	.373	.141	.169	.081
		Sig. (2-tailed)	.000	.005	.001	.105
		Interpretation	Weak	Very Weak	Very Weak	Very Weak
	HF8	Correlation Coefficient	.154	.242	.186	.225
		Sig. (2-tailed)	.002	.000	.000	.000
		Interpretation	Very Weak	Weak	Very Weak	Weak

Table 4.52: Spearman's rank correlation coefficient matrix

Author has used IBM SPSS to generate Spearman correlation matrix and applied the Author has used IBM SPSS to generate Spearman correlation matrix and applied the coefficient values from table 4.52 above to study the relationship between smart home security awareness and access control in smart home environment. Table 4.53 below shows the output.

Variables	Question No.	Relevance / grouping	Group
AU1	Q11	Awareness about device authentication before use	Awareness
AU2	Q12	Awareness of sharing devices with others	Awareness
AU3	Q13	Awareness about sharing health data	Awareness
HF8	Q46	Awareness about cost of negligence	Awareness
AR1	Q15	Sharing data with government agency	Access Control
AR2	Q16	Giving control to government agencies in emergency	Access Control
AR3	Q17	Giving control to government agencies in crime investigation	Access Control
AR4	Q18	Need of role based configuration for guests	Access Control

Table 4.53 Group of variables used in correlation analysis

On the basis of the Spearman correlation coefficient test statistic result, it is observed that the value of correlation coefficient r_s is non-negative and less than .300 showing that there is no significant relationship between awareness on smart home security and the access control used in smart home environment.

Therefore null hypothesis is accepted and alternate hypothesis is rejected.

H_o: Accepted } **Spearman correlation coefficient $r_s < .300$**
H_a: Rejected

Statistic test result of Spearman's correlation coefficient shows that the security awareness of smart home users is not associated with the access control in smart home environment.

4.4. Summary of the Hypothesis:

Hypothesis	Statement of Null Hypothesis	Test Applied	Status of Null Hypothesis
Hypothesis 1	Smart home users are not fully aware about the data security features of smart home environment.	Kolmogorov Smirnov Test	Ho Accepted
Hypothesis 2	Smart home environment are not significantly vulnerable to hackers, if not configured properly	Chi-Square test of significance	Ho Rejected
Hypothesis 3	The security awareness is not directly related to the access controls of smart home system and devices	Spearman's correlation coefficient	Ho Accepted

Table 4.54 Summary of the Hypothesis

4.5. Conclusion

Hypothesis test result based on the survey questionnaires reveals following about privacy and security issues of smart home environment.

a. Users in smart home environment are not aware about the authentication, authorization, confidentiality, integrity availability, ease of use, trust and human factors related data.

b. Data shows users ignorance in the areas of device security, its authentication and network security related information. Users were not aware about where and how there data are stored, and how device unresponsiveness can be dangerous as hackers steal the data/information by making device unresponsive.
c. Users are not fully aware about criticality of unauthorized access of smart home devices through virus, worms, DoS attack.
d. Smart home environment is prone to attack by hackers resulting into breach of confidentiality, integrity, availability, ease of use and human factors.
e. Data related to smart home security shows that users privacy can be compromised if the number of devices collecting the users data increases.
f. Not putting central control unit of smart home environment securely can result into compromise on safety and security.
g. User's perception on financial/online transactions is inclined towards the network security offered to them through the smart home device or network service provider.
h. Users have admitted that data loss/ information leak is irreparable; network and device related privacy and security is a concern.
i. Device authentication and authorization are related and play very important role in dealing with the privacy and security in smart home environment.
j. Users have admitted the necessity of authenticating the data source, data sharing and carelessness on data management.
k. Users are aware about the importance of sharing data with government, law making agencies during emergency and they have agreed for data exchange even after knowing the security breach.

Smart home users are aware about the security features, vulnerability of smart home environment from hackers and also about the smart home access controls.

But, configuring the smart home devices properly, regular updates of security patches in smart home devices are must to avoid virus attack, setting up profiles for different smart users, setting roles/privileges for device and specifying what data the device can capture can make smart home ecosystem more secure.

Author has validated the proposed conceptual model Safe@Smarthome in the last chapter and has presented more findings from this research work.

CHAPTER 5
FINDINGS, CONCLUSION, SUGGESTIONS AND FUTURE SCOPE

CHAPTER 5

FINDINGS, CONCLUSION, SUGGESTIONS AND FUTURE SCOPE

5.1. Introduction

Indian smart home market is expected to reach US$13574 Million by 2026 at CAGR 29.8% (Statista Research April 7 2021). This data seems attractive for smart home enthusiast, but, the adoption of this system depends on many factors including but not limited to the safety and security of smart home environment. Past researches have revealed that lots of smart home implementation had resulted into failures due to security breaches. Author has already discussed this issue in the literature review section.

In this chapter various findings from the data analysis performed on the survey questionnaire is presented. Author has carried out the assessment of security and privacy issue in smart home systems which are using bigdata analytics.

It is important for the readers to please be clear with the fact that author has not used big data, related tools and big data analytics anywhere in this research. But, the entire research and hence the results are based on the smart home environment which are using big data and analytics. In order to give smart home users better experience of usability, service providers' makes use of big data analytics on the data (Big data) collected through smart home devices.

Therefore, the entire research and results are based on assessing the privacy and security issues of smart home environment.

This chapter will contain detailed findings on the questionnaire survey conducted by the author. Conclusions for smart home enthusiast and most importantly validation of the conceptual framework Safe@Smarthome using case based methodology. Finally the chapter ends with a limitation of this research and future scope of research in this area.

Some generic **findings from literatures:**

- Actual systematic solutions to enable the evaluation of risks in smart home environments are in high demand. Without such measures, the deployed security solutions risk fails to achieve the smart home automation systems desired security and privacy goals.

- There is a widespread demand for security to be included while displaying smart home. For limiting the threats posed by IoT-connected houses, security in design is critical, particularly in terms of malware mitigation.
- There is a need for more information on the threats to user privacy. Because the information generated within the smart home frequently is of a personal character and thus must be regarded as sensitive, exposure to privacy breaches requires attention to highlight the potential intrusions to the house's personal domain.
- The smart home security market is fragmented, indicating the need of best practices for end-users and policy measures in the form of technology standards for systems and service providers.

5.2. Key findings on smart home users:

The data collected through a survey questionnaire from 396 smart home users characterizes following attributes regarding smart home privacy and security:

- The majority of smart home users, approximately 30%, are from the age group 31 to 40 years. Other age categories range of 18-30 years, 41-50 years and 51 years above have almost equal distribution of approximately 23%.
- 96% of the respondents are holding graduate degree and above whereas only 4% are non graduates. It is likely that majority of smart home users are well qualified.
- A large segment of users (58%) comes from business family having monthly income in the range INR 1.5 Lakh and more (24%). There is a likelihood that smart home implementation cost being a major factor. People having handsome income are more desirous of having secured home and privacy.
- When it comes to the maturity level, majority of smart home users (~43%) have been using it from last 1 to 6 years. Indicating that the technology is still new among adopters. It still needs to see the maturity level.
- Utilization of smart home system is maximum (~37) in the area of home security followed by energy conservation (~30). This gives a positive direction to this research. As the role of privacy and security is a major concern in smart home ecosystem.

- Devices related to smart home security contributes to 79% of the total smart devices in use by the users. This 79% gadget includes surveillance cameras, smart locks and wireless speakers.

5.3. Findings on the assessment of smart home privacy and security using big data analytics

As stated in the introduction, this research has not involved the use of big data has not used big data, related tools and big data analytics anywhere in this research. Instead, the entire research and hence the results are based on the smart home environment which are using big data and analytics.

Findings are classified into the metrics of two broad categories – smart home security and privacy.

This research work has not explored the cause and effect of the metrics associated to smart home privacy and security, but, the major thrust is on assessing it so that take it can be taken forward for analysis and further recommendations.

Presented below are findings on the outcome of assessment of smart home privacy and security.

1. **Assessment on security related metrics:**

   a. **Authentication:**

   99% smart home users are aware of the relevance of trusted data source and 96% knows the severity of smart home data breach owing to data sharing, indicating that the users are aware of data authentication. Though, this knowledge could be a matter of coincidence as only 14% users were having professional qualification. Contrary to this 57% are ready for sharing data with research agency for improvements in existing services and astonishing 81% during extreme emergency condition like crime detection. This is indicative that though, users knows about data authentication but needs to be enriched on improving the smart home security by restricting device access from anonymous source.

   b. **Confidentiality:**

   87% of the smart home users are concerned about security of their personal data over cloud and 79% have claimed that unregulated data collection by smart home devices may lead to security breach. The users know about confidentiality but may be ignorant on controlling the data by the service provider.

c. **Integrity:**

More than 72% of the smart home users know that data encryption can prevent data manipulation and 85% knows that smart home device verification is important for ensuring data reliability. Users are aware of integrity issue, but, whether they know how to ensure is also important.

d. **Availability:**

More than 93% of the smart home users are aware of the seriousness of data loss, 87% knows the importance of smart home device security and the importance of its becoming unresponsive. Assessment can be made that users knows about the importance of data and device availability.

e. **Access control:**

75% of the smart home users are aware about the importance of device password and relevance of security patches. 99% of the users want to be notified on device password change, malfunctioning or abnormality. Data. This metrics could be of immense use for the device service provider as the features need to be an integral part of the service offered.

2. **Assessment on privacy related metrics:**

a. **Authorization:**

Smart home users do not want to authorize the external users to breach their privacy and the same is visible in the responses. 70% users consider data privacy is important, but, 90% are ready to authorize government agencies during disaster management and crime control. Need for setting the role based access of smart home devices is important for 78% smart users, similarly 90% of users would like to have high levels of security levels for their personal area network. This is important for new smart home users and device manufacturer/service provider to give due importance to authorization and its control.

b. **Trust:**

Trust is an important element especially when the system under study is an automated system. Trust on network security is important for more than

70% of the smart home users. More than 71% of the users have trust on that branded smart home devices and 79% have trust that such devices can safeguard their smart home privacy. It is worth noticing that more than 91% smart home users expects the smart home device manufacturers to provide built-in security features.

3. **Ease-of-use related metrics:**

   Ease-of-use is considered very important for adoption of any system. Author has included the privacy and security related ease-of-use metrics to assess smart home users on this issue. The result shows that 66% users need user friendly device management, 49% users' need easy for managing device security.

4. **Human factors related metrics:**

   A software based system is in complete without assessing the role of human factors. Therefore, author has included privacy and security related human factors metrics to assess smart home users on this issue. The result shows that 94% of the users are concerned about safety and security of home. More than 90% of the users are aware that information leakage, identity theft, data breach, access of open Wi-Fi for remote smart home management and virus attacks are major threats on smart home privacy and security.

5.4. Addressing research questions

In this research work the questionnaire will address following aspects of a smart home environment:

- **Which are the IoT devices most commonly used by smart home users?**
  CCTV camera for surveillance, smart locks, video doorbells, wireless speakers, smoke detector, smart heating ventilation and air conditioning (HVAC) and smart television.
- **Are smart home users aware of the private information they share while using IoT devices?**
  Users are not willing to share data generated from smart home devices for sales promotion or advertisement. However, they are ready to share the in case of disaster, emergencies and for crime detection.
- **What are users' perceptions on general security?**

Smart home users believe that technologies will help protect their personal information. For instance, both Apple and Google are regarded as secure gadget service providers who strictly adhere to industry best practises for security and privacy. That is why smart home owners prefer to buy branded smart devices over non branded. Users are very well aware about the cyber-attacks and its ill consequences

- **Are users willing to share private data/information?**

  Knowing the severity of dangers associated with information theft, smart home users are not willing to share their smart home related personal data. However, they are ready to share only health related data with care takers and/or relatives.

- **Do smart home users have any knowledge about the data storage and devices safety?**

  Smart home users are aware that their data is stored over cloud. They demand their smart home device manufacturers to be more transparent in disclosing how much archived data is retained. For smart home device security user prefers to get security patches updates from the device manufacturers to fight hackers, virus attacks.

- **Do users have any idea related to the risks of using IoT devices?**

  Smart home security is given top most priority by the users. They are aware of risk associated with financial transaction owing to data breach at device level as well as network service provider. Relevance of keeping smart home devices securely is also known to users. Users expect that smart device manufactures should provide built-in security features to get alerts and notifications in case of device malfunctioning and for security breaches.

- **What are the recommended practices to follow in order to ensure protection of privacy and security in smart home environment?**

  - Role based assess control on smart home device
  - Personal Wi-Fi network security to be configured at high level of security
  - Ensure that smart home service provider stores data using standard encryption.
  - Smart home devices are to be kept at physically secured location

- Smart device must support alerts / notification of abnormal system functioning
- Avoid public Wi-Fi for remote access of smart home system/devices
- Ensure to buy branded smart home devices/ appliances manufactured using international specification
- Make yourself abreast with underlying technology supported by your smart home system.

5.5. Suggestions on smart home privacy and security:

- **For end-user**
  - Use smart devices and/or systems from reputed vendors/ manufactures
  - Change device default settings and ensure to change passwords periodically. When user performs the settings of their smart devices, they can take the opportunity to make necessary modifications to make the devices more secure. They should change default or easy to guess passwords immediately, and use unique and strong passwords for multiple accounts. While setting up smart devices, users should avoid using personally identifiable information (PII), especially while carrying out router settings.
  - Users should consider implementing network segmentation for certain smart home devices and isolate them from the smart home network. This is especially needed for vulnerable devices that cannot be patched and yet cannot be replaced or removed by users for whatever reason.
  - Monitor the device on a regular basis to ensure proper operation, detect malware, and detect integrity issues.
- **For smart home device manufacturers and service providers**
  - Users believe that smart home device manufacturers could do a lot in the area of device security and transparency in data gathering,
  - Timely security patches and firmware updates are two initial actions users can take, since updates are usually related to security issues. Users can opt to enable the auto update feature on supported devices to ensure that updates are applied as soon as they are available.

    - Training programs on users awareness on smart home device- Customers may not have interest in paying more for a safer product due to this lack of security knowledge.
    - Device manufacturer should monitor the device on a regular basis to ensure proper operation, detection of malware and device integrity related issues.
    - Device manufacturer should conduct regular audits and evaluations of smart device security features to ensure that they are functioning properly. Conduct penetration tests at least twice a year.
- **For government authorities**
    - Government should periodically review the legal and compliance regulations and requirements related to vendor's liability in ensuring smart home users data secure and private. Also, since technology is improving at very rapid pace, the compliance requirements need to be reviewed periodically.
    - Review the audit findings for compliance regulations and requirements.

5.6. Proposed Framework – Safe@SmartHome

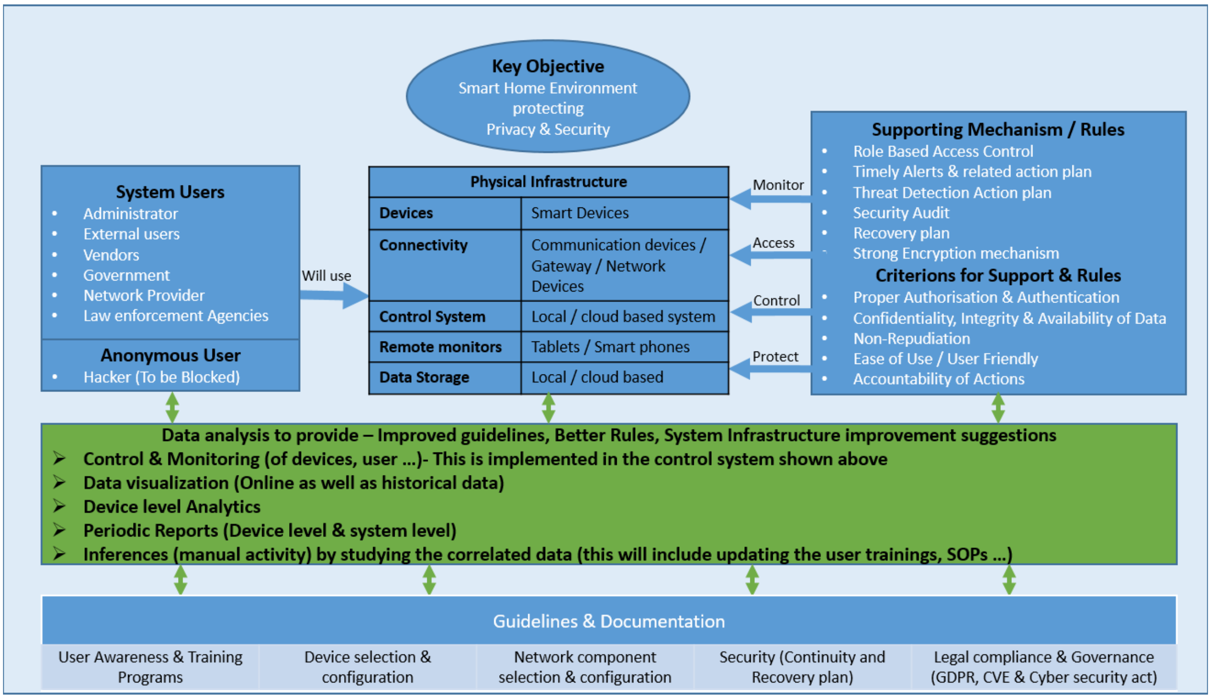

Key Objective
Smart Home Environment
protecting
Privacy & Security
System Users
Administrator
External users
Vendors
Government
Network Provider
Law enforcement Agencies
Anonymous User
Hacker (To be Blocked)
Will use
Physical Infrastructure
Devices
Smart Devices
Connectivity
Communication devices / Gateway / Network Devices
Control System
Local / cloud based system
Remote monitors
Tablets / Smart phones
Data Storage
Local / cloud based
Monitor
Access
Control
Protect
Supporting Mechanism / Rules
Role Based Access Control
Timely Alerts & related action plan
Threat Detection Action plan
Security Audit
Recovery plan
Strong Encryption mechanism
Criterions for Support & Rules
Proper Authorisation & Authentication
Confidentiality, Integrity & Availability of Data
Non-Repudiation
Ease of Use / User Friendly
Accountability of Actions
Data analysis to provide – Improved guidelines, Better Rules, System Infrastructure improvement suggestions
Control & Monitoring (of devices, user …)- This is implemented in the control system shown above
Data visualization (Online as well as historical data)
Device level Analytics
Periodic Reports (Device level & system level)
Inferences (manual activity) by studying the correlated data (this will include updating the user trainings, SOPs …)
Guidelines & Documentation
User Awareness & Training Programs
Device selection & configuration
Network component selection & configuration
Security (Continuity and Recovery plan)
Legal compliance & Governance (GDPR, CVE & Cyber security act)

Figure 5.1 Proposed Framework Safe@SmartHome

A framework Safe@SmartHome is proposed by the author after going through the literature review and analysis of survey questionnaire. This framework is divided into 5 modules namely System users, Physical infrastructure, Supporting mechanism, Criteria for support & rules, Data analysis module & finally Guidelines for protecting privacy & security

Security is the first line of defence for all activities performed by users and administrators. These keys describe the control system's essential principles. These principles have the purpose of providing good and secure access to the system. The availability of data for use, the detection of the source from which data was obtained, and user and administrator authentication and authorisation. A sample is included in the supporting mechanism. Mechanism for ensuring the safety security plan's implementation.

5.6.1. Users

5.6.1.1. **System users** – Smart home system can be exposed to different internal as well as external users. Smart homes would need to provide information and services customized to the circumstance of the user.

5.6.1.2. **Administrator** – System administrators' plays very important role in overall designing and implementation of system management. He ensure safe system and application authentication and resource authorisation in compliance with established policies.

5.6.1.3. **Vendors** – Device vendor The IoT system management agency manages processes such as configuration of systems and fault-management services, providing access to the various users.

5.6.1.4. **External Users -** Some others users may be the guest/Friends to whom the temporary Access need to be provided in some of emergencies. With the right security system in place, guest access to home will operate smoothly.

5.6.1.5. **Government** - Local governments may require to have access to system improve services based on smart home data analysis.

5.6.1.6. **Law enforcement Agencies** – Law enforcement agencies may need to have access to smart home system for crime investigation.

5.6.1.7. **Network Service provider -** The network provider that make available the network service.

5.6.1.8. **Anonymous user / Hacker** – Hacker is a person who uses his or her ability to obtain unauthorized access to systems or networks to commit crimes. For example, a hacker can steal information to harm people through identity theft, damage or bring down systems and then keep those systems hostage to gather ransom. Main objective is to block the access to the hackers and protect the users' privacy.

5.6.2. Physical infrastructure

5.6.2.1. **Smart devices** – A smart devices are an electronic devices, typically connected via various wireless protocols such as Bluetooth, Zigbee, NFC, Wi-Fi, 4G, etc. Smart devices has unique functionality. Types of IoT devices range from basic, small sensors to massive, complex systems such as Smart locks, Security camera, Thermostat, Voice assistance, Robotic vacuum cleaner, Music system, Smart TV with thousands of IoT devices. IoT devices need to be protected from DOS attacks, unauthorised access & physical damages.

5.6.2.2. **Communication Devices/Gateway / Network devices** - The IoT Gateway is one of the essential elements of this ecosystem. It handles all communication with all sensors and remote connexions, like the Internet, applications or users.

5.6.2.3. **Data storage devices** – Data is an incredibly valuable commodity to the world today. Smart home system should collect and store following types of data

- Data from sensors (e.g. CCTV footage)
- Process alerts (based on data from devices) and system alerts (based on Monitoring the system components)
- System image for easy recovery (from partial or full damage).

5.6.2.4. **Control system** - A Smart home automation system will monitor & control all sensors, networking components (using predefined configuration). The devices / sensors may be connected using various possible networks (Wi-Fi, LAN …) and using various possible protocols (Bluetooth, ZigBee …). It will also allow remote connectivity (from internet using smart devices like mobile) for control & monitoring the system. This will be typically a local PC based system (in future it can also be a cloud resident system)

5.6.2.5. **Tablet/Smart Phone** – These will typically be smart phones with built-in Applications to enable remote connectivity. Occasionally a PC can also be used (connected over the internet). The user will login to the system using these devices for performing various functions of monitor, control & configuration.

5.6.2.6. **Supporting Mechanism**

By their very design, the supporting controls are ubiquitous and interrelated with many other controls. Supporting mechanism systems may be designed to defend against various types of threats. This mechanism involves Protection system with a mixture of hardware, firmware and applications. These all majors should work together to secure confidential and sensitive data, information and system.

5.6.2.7. **Role Based Access Control** – Means Separate user group as per facility. This will help to protect the data integrity and confidentiality. The efficiency and strength of access control rest on the accurateness of access control decisions (e.g. how to configure security rules) and the strength of access control enforcement (e.g., software or hardware security).

5.6.2.8. **Threat Detection Action plan** - The most critical aspect of Smart Home Protection is threat detection and response. It is necessary that system should quickly detect threat and next step is the response. Threat responses should be prepared in advance to allow for decisive action.

5.6.2.9. **Timely Alerts** – Real time notifications to your smart phone or tablet to remote location makes the home smarter. When you're at home or away from home, instant to your smart phone. Weather alerts, power failure notifications or security alerts are set directly on your smartphone to keep you updated at all times.

5.6.2.10. **Intrusion Detection system** (IDS) – It is essential to detect suspicious attempts made by intruders, so that actions can be taken instantly.

5.6.2.11. **Intrusion Prevention system** (IPS) – The IPS provides prevention of intrusion is to create a defensive methodology to network security in order to identify and respond to potential threats quickly. Thus, intrusion prevention systems are used to examine network traffic flows to find malicious software and to avoid exploits of vulnerability.

5.6.2.12. **Security Audit - T**he auditing of security related occasions and the monitoring and tracking of system anomalies are key elements in the after-the-fact exposure and recovery from, security breaches.

5.6.2.13. **Recovery plan -** Recovery **plan** aims to rapidly coordinate the resources needed to rebuild data and information systems after a disaster. A disaster may be defined as a sudden occurrence, like an accident or natural disaster, resulting in wide-ranging, harmful damage. Same plan/ procedures can also be used to recover the system after external virus/ malicious attack causing partial or full damage.

5.6.2.14. **Procedure to prevent LOV & LOC: LOV (Loss of view)** means inability to monitor the system due to issues like non-availability of network (which would prevent from logging to the network / system to view / monitor the same). **LOC (Loss of Control)** mane inability to control / configure the system due to issues like non-functioning of the controlling unit. The measures like redundant system architecture (network and / or control system) will help to avoid LOV / LOC

5.6.2.15. **Strong Encryption mechanism –** Protected communications use data encryption methods e.g., virtual private network(VPN), Internet Protocol Security [IPSEC] Protocol, and deployment of cryptographic technologies like Data Encryption Standard [DES], secure hash standard, and escrowed encryption algorithms such as Clipper to decrease network threats such as packet sniffing, wiretapping, or eavesdropping.

5.6.2.16. **Criteria for support and rules –** Is nothing but the objectives to be achieved.

5.6.2.17. **Authorisation & authentication** - Authorisation is the function of specifying resource access rights / privileges, which relate to information security and computer security in general, and access control in particular. More formally, "authorizing" means defining a policy on access officially. Authorization is applied only after proper authentication. **Authentication** is the process of verifying the identity of a person or device. Authentication technique typically includes user name & passwords / PIN (Personal Identification Numbers). New authentication technologies that provides more effective authentication include Token, OTP, Smart Card, Digital Certificate, and Kerberos.

5.6.2.18. **Confidentiality, Integrity & Availability –** Confidentiality mean protecting information from being accessed by unauthorized parties. Confidentiality ensures that the Sensitive / relevant information is not presented to unauthorized entities (user or device) and users with lesser authorization / credentials. **Integrity** means maintaining the accuracy, and completeness of data. It is about protecting data from being modified or misused by an unauthorized user / user with lower credentials. Integrity involves maintaining the consistency and trustworthiness of data over its entire life cycle. It also ensures that processes are in place to detect any such changes in data & restoring the original data. Availability means that the system/Data should be made available on demand. Resolving differences between hardware and software, along with routine maintenance, is key to keeping devices up and at their disposal.

5.6.2.19. **Non-repudiation** - It means putting measures in place that will prevent denial of service (related party denying they received or agreed to a transaction). Non-repudiation is to detect that the source of data is confirmed with proof of delivery and the receiver of data is confirmed with proof of the sender's identity

5.6.2.20. **Accountability** - It **means** assigned responsibilities for system functionality. It ensures that procedures are in place to track acts / events back in time to the users, programs, or procedures that performed them (in order to maintain responsibility for actions or omissions). It is required to maintain transparency. System would not be regarded secure if it does not have accountability. Without such provisions it will be difficult to know who is responsible, what happened or did not happen on the system. In the context of information management, transparency is primarily provided by reports and the audit trail.

5.6.3. Data analysis

The individual devices will have their own formats/values for sharing the information. Also it is not same from all the devices. Hence the data collected from these devices (field data & configuration data) is in heterogeneous format. Hence this data will be similar to big data. Big Data tools (like Hadoop, Map Reduce) can be used to analyse the data. Following facilities are expected

- Control & monitoring – The main goal of this function is to provide useful information in real time so that damage can be prevented. This will be done in the control system

- Visualization – to present the data in various formats (like data between predefined period, data around alert received from same device or correlated device)
- Reports – To generate period data collects (like alerts generated per day per device, data from each device for predefined period …) also to capture the device configuration. Reports of user activities

Following are benefits of individual facilities

- Control & monitoring
  - Possibility to take Immediate actions to prevent or minimize the damage
- Visualization
  - To assess wear & team of the device (need to replace the device or to perform maintenance)
  - To assess and define season specific settings
  - To monitor user activities and check for system hacking
- Reports
  - To define system health status (functionally correct operation) of the system
  - To determine need of device reconfiguration / maintenance activities (in case of multiple false alarms)
  - To Recover the last good configuration (in case of need of system recovery)
  - To determine the need of reconfiguration of user access / authentications. This can also help to determine if system was hacked and need to be recovered using last known good configuration

The Study of data can also be used to update the user awareness programs, good practices for device configuration. This data can also be shared with authorities to help capture possible intruders, to come-up with improved legal framework to penalize the guilty people (like hackers, Intruders, thieves)

5.6.4. Guidelines & Documentation

Lastly this framework will provide Guidelines and Documentation to the Smart home user. Following are the Guideline.

- Device selections and related configuration
- Configuration details
- Users Role Configuration

- Actual Recovery plan
- Network components selections
- User awareness training program
- Security legislation, regulatory guidelines to ensure compliance and Governance with the Information Assets

5.7. Scope for future work in Safe@Smarthome

The section 5.7 defines the framework for SafeHome. It defines multiple components / modules involved in defining the smart home. The main categories are

- Smart devices used
- Network for connectivity of devices and the system
- Control system
- Users
- Data storage

The technology is improving / evolving at very rapid speed. This will make thing possible that are considered impossible with today's technology.

We will discuss the possible enhancements for each of the modules defined above

5.7.1. Smart devices (scope of device manufactures)

- The devices will be smarter & intelligent. They will communicate with each other (in absence of the control system) to take decisions in case of emergency (e.g. smoke / fire detection system will directly communicate with the water management system in case of smoke detection or fire detection). This will be in addition to the normal communication with the control system. This will to take faster actions to optimize the loss that may occur. This will help the system to continue in case of non-availability of the control system for shorter duration
- The devices will support multiple communication protocols that will help to improve interoperability
- Possibility of embedding multiple sensors in single device making the device multifunctional. This will help reduce number of devices to cover same requirements
- The devices will be powerful enough to store the data within themselves, including the data encryption. This will help to store data for larger duration. This in future will help the future application for more detailed analysis

- The devices will work on low power requirement there by reducing over-all energy requirement that will help to reduce cost of operation. It will be likely that the required power is generated using solar power
- With assured encrypted communication the manufactures will be able to update the firmware, security patches making them more robust

5.7.2. Networking & device connectivity (scope of service providers)

- Stronger built-in security configuration making it difficult for hackers to take control of the system
- Higher speed of connectivity and support for larger distances will help to reduce the interconnecting intermediate devices
- Everybody is communicating in wireless

5.7.3. Control system (scope of service providers)

- More use of technology of Artificial Intelligence & Machine Learning algorithms will make system more powerful & intelligent
- Completely distributed system (each device having its own function control algorithms) making it difficult for hackers to take control of the system
- Improved predictive algorithms will enhance ability to anticipate failures. This will improve the system uptime.
- Self-correcting systems

5.7.4. Data storage (scope of service providers)

- Ability of storing large amount of data in relatively small space will help analysis using more data-points
- Improved cloud storage (with faster communication speeds & security aspects) will reduce need of local storage. This will further reduce system sizing / footprint.

5.7.5. Applications for data analysis (scope of service providers)

- Single tool will have ability to interpret data from more number of devices.
- Improved AI & ML algorithms will provide better analysis, early detection, predictive features to anticipate failures
- With appropriate security configurations these tools may interact with systems & devices for online corrections, improving the security & functionality. There

may be a possibility of communicating with government / law enforcing agencies in case of any illegal findings, emergency situations

- Better understanding of user interactions will help to improve training material, operating procedures.

5.7.6. SafeHome as service

- Software as a service (SaaS) is an established offering in the service industry. This concept can also be extended to the services for smart home. The agencies can provide independent consulting services for smart home configuration (including selection of devices, networking & security configurations) bundling with state-of-art data analytics tools. Following figure gives a typical framework for suce service industry.

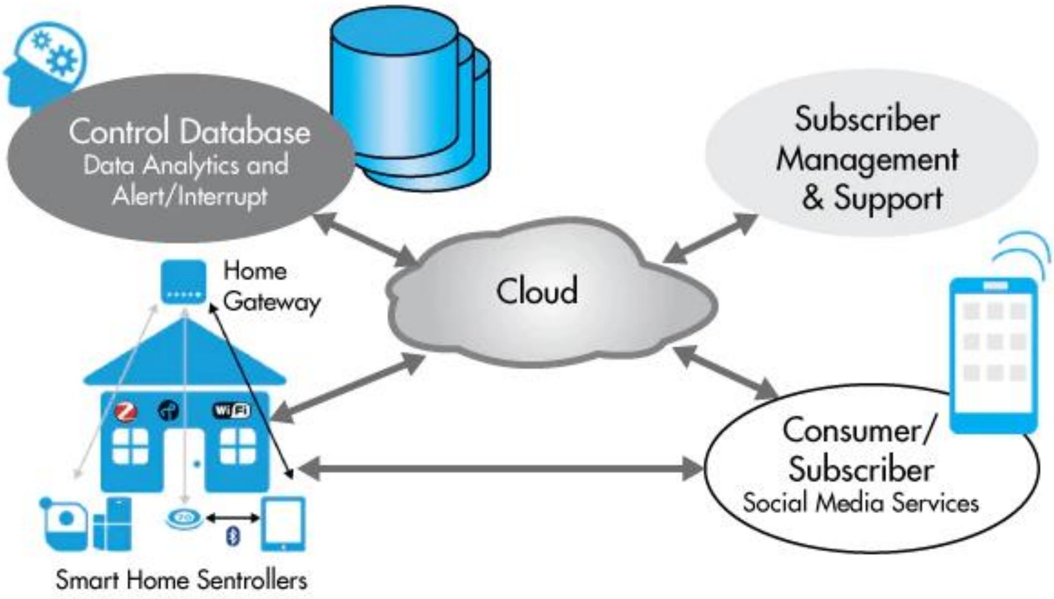


Figure 5.2: Smart home system

Source: https://images.app.goo.gl/q6qtuopx8HQfBCp67

5.8. Validating a framework Safe@Smarthome:

This section constitutes the final stage of assessment of smart home privacy and security. The proposed conceptual framework is examined using case based approach. The purpose is to verify whether the proposed framework is viable and acceptable in smart home ecosystem. To complete this portion of work a separate questionnaire comprising 7 questions on smart home system privacy and security were asked. Respondents were smart home device manufacturers and service providers. Interviews are recorded for future use and the same is retained in hard copies. Total 9 subjects were interviewed and the responses received are analysed to converge to a concrete conclusions. Respondents are from prestigious organizations like Tata Honeywell, L&T Infotech, Smato, Safehouse, Prosonic to name a few.

As it is important to look towards the privacy and security of smart home from manufacturers and service providers perspective, this part of research work could be of immense use for various stakeholders of this ecosystem.

Given below are the question, responses and inference on Safe@Smarthome model. In some instances redundant responses were received, such responses are considered only once while presenting it to the readers.

5.8.1. What is the importance of "Role based access control" in limiting undesirable access to smart home device?

"It's a high security technology that keeps all smart home devices safe."

"Role based access control gives more security to the system, it controls unwanted access to smart home system."

"It is helpful for audit and track of history"

"Avoids unwanted access to smart home system"

"Useful in remote management of smart home ecosystem"

"It is useful in prevention of intrusion, unwanted device access and its management."

"It is useful in reducing overall exposure and levels of vulnerability for cyber attacks. Users can set the permissions for carrying out various actions in a smart home ecosystem."

The responses received are enough to consider that the respondents have accepted that Role based access control (RBAC), smart home devices authorization and access control is important for security of smart home ecosystem. Past researches have put these feature under smart home security. Smart home manufacturers and service providers have agreed that for smart home security role based access control, device authorization and control is a desired feature. This is presented under the supporting mechanism and rules and criterion for support and rules in Safe@Smarthome model.

5.8.2. Do you receive request from smart home users to provide them information related to unauthorized access of smart home device?

"Unauthorized device access is prevented by updating smart devices and using firewalls provided by us."

"As roles and access are defined in the system, unauthorized access is denied and notification is forwarded to the users. Only authorized users are approved to provide access to other users."

"Yes we get request from smart home users for unauthorized access of device. But, only authorized users can provide access to other users. Periodic update of device firmware and firewall can prevent unauthorized access."

"Yes, as smart home users are very much careful about the security of their smart home system."

The responses received are suggesting that timely alerts and related action plan as well as authorization and access control of smart home devices is considered important for security. Smart home device manufacturers are in support of this feature of Safe@Smarthome framework model.

5.8.3. Do you think it is important to monitor 3rd party intrusion on smart home device?

"It is important to monitor third party intrusion attempt to maintain smart home safety and security. During large gatherings at home such kind of attempts are very common."

"Yes it is important to monitor third party intrusion attempts to secure smart home environment."

"It is required and to avoid such intrusions monitor unnecessary usage of smart home devices, control/change the device password, use card/biometric based device authentication."

"Yes, in order to safeguard the smart home ecosystem from intruders and to make smart home safe and secure."

These responses received from manufacturers and service providers indicates the importance of threat detection, its mitigation and non-repudiation of smart home system.

The same is presented by author under supporting mechanism and criterion for support and rules in Safe@Smarthome model.

5.8.4. Do you update the security patches of your smart home devices regularly? What role does it play in smart home security?

"Yes we do provide periodic updates of security patches for most of the smart home system controllers we sell. It is important for improved smart home security."

"Managing security patches is a challenging task, especially for vendors. But it is important to apply patches as soon as they are released. Device settings, credentials, firmware updates, versions and recent patches should be noted."

"Security patches should be updated on smart home devices for better security and updated technology access. Improper patch updates exposes the entire smart home system to hackers."

"Yes, we upgrade the patch on a regular basis, and it plays a significant role in increasing smart device security because each version has its distinct increased security feature."

"Yes, we update the security patches for enhancing security on regular basis since each update will have a different enhanced security feature."

"Yes, we do it regularly for device protection and protecting information from intrusion/ attack.

We do check and provide patch updates every week or as per OEM's recommendation."

The responses received shows that device security audit is important for smart home security. Author has included this issue of smart home privacy and security is included in Safe@Smarthome.

5.8.5. Does your smart home device withstand hackers attack and network security breach attempts?

"Not experienced hacker attacks but hope that they can withstand the attack with the available in-built security."

"No, hackers can change the configuration or reset the system only."

"The built-in security in the home devices and timely updates of the same reduces the possibility of hacking."

"Yes, with proper security updates in place the device can withstand hackers attack. But, the system needs to be up to date on security front."

The responses received is indicative that smart home device integrity. Threat detection mechanism and related action plan is important for security of system. This is included in the model Safe@Smarthome.

5.8.6. Do you use any data encryption technique while sending smart home data over cloud?

"While transferring data to the cloud, we utilise encryption to ensure data security".

"We utilise encryption to ensure data security when moving data to the cloud. Any type of hacking committed while transmitting data might result in an offence and the liability is of service provider."

"We do use encryption method to maintain data security while transferring data on cloud. It is important for any user to use encryption technique so that data can be protected. Any kind of hacking performed while transferring the data, can lead to crime."

"Encryption method was default and didn't try utilising a separate method."

"End-to-end encryption method is being used."

"Encryption method is default and didn't try using a separate method."

"We use the encryption method provided by the OEM's."

The responses received by different manufacturers and service providers have consented on the significance of strong encryption mechanism. Responses suggests use of encryption technique is important for smart home data security.

Author has included this feature of smart home system in Safe@Smarthome model.

5.8.7. Do you offer simple and easy to use device management features to the users?

"Our smart home devices are user friendly, easy to install, highly protective. Device management configuration services are used for all the electronic devices from point of view of confidentiality and privacy. Currently we are providing device management configuration for products electronic security technology products."

"The services offered are user friendly."

"The system is user friendly."

"All the smart home devices configuration management is user friendly."

"Yes, user friendliness is there and information. Configuration is through dashboards."

"Yes, it is there as it supports ease of use and reporting."

It is clear from the responses received that smart home device manufacturers have agreed that ease of use is important for smart home management. If the end users are not provided with easy to use device and configuration management, users may restrain themselves from enabling certain options due to complicated operation procedure. This issue is important for smart home security and is included by author while proposing Safe@Smarthome.

5.9. Connecting Safe@Smarthome and smart home privacy and security:

Author has included the factors related to smart home supporting mechanism and the criterion for support in the proposed model Safe@Smarthome..

The model includes following factors:

1. Role based access control
2. Security alarms and related action plan
3. Threat detection and action plan
4. Security audit
5. Recovery plan
6. Strong encryption method
7. Proper authorization and authentication
8. Confidentiality, integrity and availability of data
9. Non-repudiation
10. Ease-of-use / user friendliness
11. Accountability

The factors listed above falls in privacy and security related issues of smart home environments.

Case based analysis of the responses received from smart home device manufacturers/ service providers is in support of the proposed framework Safe@Smarthome.

It is worth noting that the 37 factors used in the research for the assessment of privacy and security of smart home environment using big data analytics is validated using Safe@Smarthome.

The respondents of the questionnaire survey used in this research work were smart home users and the respondents of case based research were smart home device manufacturers/service providers.

The responses of case based research is collating with the empirical results and/or hypothesis used in the research.

It also validates the proposed conceptual model Safe@Smarthome.

5.10. Research contribution

This study promises to contribute in multiple aspects

- Safe@Smarthome framework will help to standardize the system and improve adoption by smart home users
- The research and its findings is useful for future research efforts aimed at creating a more secure and private IoT enabled smart home environment.
- This research will contributes in improving smart home related IoT businesses in recognising users requirement of stronger privacy protections in IoT devices.
- The findings of the study will give academic researchers and industry experts insight into smart home users' security and privacy concerns.

5.11. Limitations of the Research

Author has found certain limitations in this research work. They are classified based on the research methodology and the coverage of research sample.

- Contacting users
    - Due to the pandemic situation few users were contacted through social media apps.
    - The participants were contacted using Google forms.

    Possible improvements for future research

    - In addition to the connect using social media, more face to face dialogues like work-shops, direct visits to individual's residence. This will help to understand the qualitative concerns / requirements (objective questions have limitations to collect such information)
- Residential / demographic separation
    - The residential location was restricted to Pune and adjoining districts of Maharashtra (urban population).

  Possible improvements for future research

    - A separate study can be conducted including smart home users that represent specific state or a representation of country. This can lead to different results.
- Variety of smart home devices
    - There is significant variety of smart home devices deployed in home environment. But, the research was restricted to more common and popular devices.
    - Smart home is a complex concept and is still evolving. No two smart homes are same in all respect. Use of smart home devices in the ecosystem varies from user to user.

  Possible improvements for future research

    - The proposed research parameters need to be updated from time to time so that more devices and associated privacy and security features can be assessed .
- Requirements and perceptions of smart home users

    - There is significant variation (conflicting at some times) in the perception of smart home users. Also their expectation from smart home is diverse.

  Possible improvements for future research

    - Future research can be done by including the smart home users expectations.

- Data Analysis
    - Big Data analytics and relate tool & technologies are not considered in this research, as generic tools (covering multiple devices) are not avialable.

REFERENCES

Journal & Articles

- Abhay kumar ray Issues, Challenges and Application of Big Data International Journal of Computer Applications (0975 – 8887) International Conference on “Computer Systems & Mathematical Sciences” (ICCSMS 2016)
- Aditya Dev Mishra Big Data Analytics for Security and Privacy Challenges International Conference on Computing, Communication and Automation (ICCCA2016)
- Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. Journal of Network and Computer Applications, 66, 198-213
- Ali Padyab and Anna Stahlbrost Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations 2018
- Andreas Jacobssona, Martin Boldtb, Bengt Carlssonb A risk analysis of a smart home automation system A. Jacobsson et al. / Future Generation Computer Systems 56 (2016) 719–733
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805
- Avirup Dasgupta, Asif Qumer Gill and Farookh Hussain (2019) Privacy of IoT enabled Smart home systems DOI: 10.5772/intechopen.84338
- Baronti, P., Pillai, P., Chook, V. W., Chessa, S., Gotta, A., & Hu, Y. F. (2007).Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. Computer communications, 30(7), 1655-1695.
- Batista, N. C., Melício, R., & Mendes, V. M. F. (2017). Services enabler architecture for smart grid and smart living services providers under industry 4.0. Energy and Buildings, 141, 16-27.
- Berrios, V. & Harvey, R. (2017). zigbee evolution continues with wireless IoT security updates.http://embedded-computing.com/articles/zigbee-evolution-continues-withwireless-iot-security-updates/ [2017-05-15] Bluetooth. (2017).
- Bryman, A., & Bell, E. (2015). How it works. https://www.bluetooth.com/what-is-bluetoothtechnology/how-it-works [2017-04-24]
- Chakravorty A, Wlodarczyk T, Chunming R. Privacy Preserving Data Analytics for Smart Homes. Security and Privacy Workshops (SPW), 2013 IEEE. IEEE; 2013. [Google Scholar]

- Chan, M., Campo, E., Estève, D., & Fourniols, J. Y. (2009). Business research methods. Oxford University Press, USA.
- Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). Smart homes—current features and future perspectives. Maturitas, 64(2), 90-97.
- Charlton, M. (2016). A review of smart homes— Present state and future challenges. Computer methods and programs in biomedicine, 91(1), 55-81.
- Chen, M., Wan, J., & Li, F. (2012). Machine-to-machine communications: architectures, standards and applications. KSII transaction on internet and information systems, 6(2), 480-497.
- Colak, I., Sagiroglu, S., Fulli, G., Yesilbudak, M., & Covrig, C. F. (2016). A survey on the critical issues in smart grid technologies. Renewable and Sustainable Energy Reviews, 54, 396-405
- Cook, D. J. (2012). How smart is your home? Science, 335(6076), 1579-1581.
- Cook, D. J., Augusto, J. C., & Jakkula, V. R. (2009). Ambient intelligence: Technologies, applications, and opportunities. Pervasive and Mobile Computing, 5(4), 277-298.
- Cook, D., & Sajal, K-D. (2004). Smart environments: Technology, protocols and applications. Vol. 43.
- Demiris, G. (2004). Electronic home healthcare: concepts and challenges. International Journal of Electronic Healthcare, 1(1), 4-16.
- Depuru, S. S. S. R., Wang, L., & Devabhaktuni, V. (2011). Smart meters for power grid: Challenges, issues, advantages and status. Renewable and sustainable energy reviews, 15(6), 2736-2742.
- Domingues, P., Carreira, P., Vieira, R., & Kastner, W. (2016). Building automation systems: Concepts and technology review. Computer Standards & Interfaces, 45, 1- 12.
- Eric Zeng, Shrirang Mare, and Franziska Roesner, University of Washington End User Security and Privacy Concerns with Smart Homes Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) July 12–14, 2017.
- Flick, U. (Ed.). (2013). The SAGE handbook of qualitative data analysis.
- Friedewald, M., Vildjiounaite, E., Punie, Y., & Wright, D. (2007). Privacy, identity and security in ambient intelligence: A scenario analysis. Telematics and Informatics, 24(1), 15-29.

- Geethumohan IOT AND BIGDATA ANALYTICS APPROACH USING SMART HOME ENERGY MANAGEMENT SYSTEM (2019)
- Gill, K., Yang, S. H., Yao, F., & Lu, X. (2009). A zigbee-based home automation system. IEEE Transactions on Consumer Electronics, 55(2).
- Grimaldi, D., & Fernandez, V. (2016). The alignment of University curricula with the building of a Smart City: A case study from Barcelona. Technological Forecasting and Social Change.
- Hacking lightbulbs. PhD student's research earns international media attention. https://www.dal.ca/news/2016/11/07/hacking-lightbulbs--phdstudent-earns-international-attention-fo.html [2017-07-04]
- Harper, R. (2003). Inside the smart home: Ideas, possibilities and methods. In Inside the smart home (pp. 1-13). Springer London.
- Hjorth, T. S., & Torbensen, R. (2012). Trusted Domain: A security platform for home automation. Computers & security, 31(8), 940-955.
- Hui, T. K., Sherratt, R. S., & Sánchez, D. D. (2016). Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. Future Generation Computer Systems.
- Incibe. (2017). Security in ZigBee communications. https://www.certsi.es/en/blog/security-zigbee-communications [2017-05-15]
- Ismini Psychoula, Deepika Singh, Liming Chen, Feng Chen Andreas Holzinger, Huansheng Ning§ Users' Privacy Concerns in IoT based Applications · September 2018
- Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, 719-733.
- Jiv chnag 2019 IoT Device Security: Locking Out Risks and Threats to Smart Homes (white paper)

  John Wiley & Sons. Creswell, J. W. (2013). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.
- Kabalci, Y. (2016). A survey on smart metering and smart grid communication. Renewable and Sustainable Energy Reviews, 57, 302-318.
- Keith Worden, William A. Bullough and Jonathan Haywood (2013) The Smart Approach — An Introduction to Smart Technologies DOI:10.1016/j.jsv.2003.12.002

- Khatoun, R., & Zeadally, S. (2016). Smart cities: concepts, architectures, research opportunities. Communications of the ACM, 59(8), 46-57.
- Korkmaz, I., Metin, S. K., Gurek, A., Gur, C., Gurakin, C., & Akdeniz, M. (2015). A cloud based and Android supported scalable home automation system. Computers & Electrical Engineering, 43, 112-128
- Kristian Beckers1 (B), Stephan Faßbender, Maritta Heisel, and Santiago Suppan2A Threat Analysis Methodology for Smart Home Scenarios feb 2008
- Kshetri, N. (2017). The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply. Telecommunications Policy, 41(1), 49-67.
- Li, Rita Yi Man; Li, Hero Ching Yu; Make, Cho Kei; Tang, Tony Bei qi. "Sustainable Smart Home and Home Automation: Big Data Analytics Approach". International Journal of Smart Home. 10 (8): 177–198. doi:10.14257/ijsh.2016.10.8.18
- Li, X., Lu, R., Liang, X., Shen, X., Chen, J., & Lin, X. (2011). Smart community: an internet of things application. IEEE Communications Magazine, 49(11).
- Lilis, G., Conus, G., Asadi, N., & Kayal, M. (2017). Towards the next generation of intelligent building: An assessment study of current automation and future IoT based systems with a proposal for transitional design. Sustainable Cities and Society, 28, 473-481.
- Lühr, S., West, G., & Venkatesh, S. (2007). Recognition of emergent human behaviour in a smart home: A data mining approach. Pervasive and Mobile Computing, 3(2), 95-116.
- Luor, T. T., Lu, H. P., Yu, H., & Lu, Y. (2015). Exploring the critical quality attributes and models of smart homes. Maturitas, 82(4), 377-386.
- Mantripajit kaur, 2016. Big Data Analytics on IOT Challenges, Open Research Issues and Tools.
- Mosannenzadeh, F., Bisello, A., Vaccaro, R., D'Alonzo, V., Hunter, G. W., & Vettorato, D. (2017). Smart energy city development: A story told by urban planners. Cities, 64, 54-65.
- Nixon, P., Wagealla, W., English, C., & Terzis, S. (2004). Privacy, security, and trust issues in smart environments.

- Oates, B. -J. (2006). Researching Information Systems and Computing. London: SAGE Publications Ltd. Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017).
- Saeedreza Arab Internet of Things: Communication Technologies, Features and Challenges (2018)
- Sage. Fortino, G., Guerrieri, A., Russo, W., & Savaglio, C. (2014). Middlewares for smart objects and smart environments: overview and comparison. In Internet of Things Based on Smart Objects (pp. 1-27). Springer International Publishing.
- Seul-Ki Choi1 Chung-Huang Yang2 and Jin Kwak3System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 12, NO. 2, Feb. 2018
- Shafiq Ul Rehman and Selvakumar Manickam A Study of Smart Home Environment and its Security Threats International Journal of Reliability, Quality and Safety Engineering Vol. 23, No. 3 (2016) 1640005
- Sharda R. Katre1, Dinesh V. Rojatkar2 (2017) HOME AUTOMATION: PAST, PRESENT AND FUTURE International Research Journal of Engineering and Technology (IRJET) 10(4) 344-346
- Simon moncrieff, Sevetha Venkatesh, and Geoff West Dynamic Privacy Assessment in a Smart House Environment Using Multimodal Sensing ACM Transactions on Multimedia Computing, Communications and Applications, Vol. 5, No. 2, Article 10, Publication date: November 2008.
- Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. 2015 IEEE 11th International Conference on Wireless and Mobile Computing,Networking and Communications, WiMob 2015. https://doi.org/10.1109/WiMOB.2015.7347956
- Surinder Kaur HOME AUTOMATION AND SECURITY SYSTEM (2016)
- V. Vimarlund1, 2, S. Wass1 Big Data, Smart Homes and Ambient Assisted Living(2014)
- Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner Assessing Users' Privacy and Security Concerns of Smart Home Technologies V. Zimmermann et al., Privacy and Security Concerns of SH Technologies 2019

- Won Min Kang, Seo Yeon Moon and Jong Hyuk Park An enhanced security framework for home appliances in smart home Kang et al. Hum. Cent. Comput. Inf. Sci. (2017) 7:6 DOI 10.1186/s13673-017-0087-4
- WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings
- Youssef Gahi, Big Data Analytics: Security and Privacy Challenges 2016

Websites

- https://www.otelco.com/resources/smart-home-guide/
- https://www.perle.com/articles/top-iot-security-vulnerabilities-2020-and-beyond-40189357.shtml
- https://cybersecurityventures.com/internet-of-things-hacks/
- https://www.alarm.com/home_automation.aspx
- https://www.varonis.com/blog/cybersecurity-statistics/#impact
- https://www.smarthome.com/
- https://blog.feedspot.com/home_automation_blogs/
- https://blog.coldwellbanker.com/category/smart-home/
- http://www.builderonline.com/tag/home-automation
- https://cis-india.org/internet-governance/files/gdpr-and-india
- https://www.gsma.com/iot/wp-content/uploads/2018/11/GSMA_Assessing-regulatory-requirements-of-privacy-management-for-members-offering-IoT-services-using-personal-data.pdf
- https://iapp.org/news/a/information-technology-rules-2021-suggest-big-changes-for-big-tech-in-india/
- https://www.thehindu.com/sci-tech/technology/internet/apps-of-16-popular-smart-home-devices-vulnerable-to-cyberattack/article36707326.ece
- https://www.bobvila.com/slideshow/the-10-biggest-security-risks-in-today-s-smart-home-53081
- https://www.techradar.com/in/news/smart-home-devices-are-being-hit-with-more-cyberattacks-than-ever
- https://www.honeywell.com/us/en
- https://www.iotevolutionworld.com/smart-home/articles/445815-iot-time-podcast-s5-ep23-honeywell-smart-buildings.htm
- https://trust.mi.com/pdf/Xiaomi IoT_Privacy
- https://www.rambus.com/iot/smart-home/
- http://www.smarterhomeautomation.com/blog/
- https://www.vivint.com/
- https://www.homeautomat.in/

- https://www.sciencefocus.com/future-technology/smart-home-the-best-automation-devices
- https://www.gartner.com/en/information-technology

Books and eBooks

1. Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems by River Publishers series in communications ISBN: 978-87-92982-96-4 (E-Book)
2. Internet of things from research & innovations to market deployment by River Publishers ISBN: 978-87-92982-96-4 (E-Book)
3. IoT for smart homes by Institution of Engineering and Technology ISBN 9781785616358
4. Handbook of Big Data and IoT Security By springer ISBN 978-3-030-10543-3 (eBook)
5. How to Smart Home_ A Step by Step Guide for Smart Homes & Building Automation ISBN 978-3-944980-12-6
6. Internet of things and big data analytics toward next-generation intelligence By springer ISBN 978-3-319-60435-0 (eBook)
7. Practical internet of things security By packt publishing ISBN 978-1-78588-963-9
8. Smart home for Dummies by Wiley Publication ISBN: 978-0-470-16567-6
9. Build your own smart home By McGraw-Hill ISBN 0-07-223013-4
10. Researching Information system and Computing by Briony J. Oates
11. Research methodology by C. R. Kothari
12. Hand book of Big data and IoT security By acedmia.edu ISBN : 978-3-030-10543-3
13. Internet of things – A handbook on approach By Universities press ISBN:978 81 7371 954 7

Reports

1. Enhancing IoT Security by internet society
2. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures(EnISA) 2017
3. IoT Safety/Security Development Guidelines. Information-technology Promotion Agency, Japan (IPA) 2016, 2017
4. Technical Report on “M2M/IoT enablement in Smart home” By MINISTRY OF COMMUNICATIONS GOVERNMENT OF INDIA
5. Survey of accountability, trust, consent, tracking, security and privacy Mechanisms in online environments ENISA
6. The market potential for Smart Homes by Joseph Rowntree Foundation 2000
7. Internet of Things (IoT) Security and Privacy Recommendations by Broadband Internet Technical Advisory Group(BITAG)
8. Security and Resilience of Smart Home Environments(ENISA)
9. INTELLIGENT EFFICIENCY - A CASE STUDY OF BARRIERS & SOLUTIONS - SMART HOMES By Connected Devices Alliance (CDA)
10. Risk Management Guide for Information Technology Systems by NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY(NIST)

Questionnaire

Dynamic Privacy & Security Assessment in a Smart Home Environment Using Big data Analytics

1. Email address * ____

2. Name of the respondent ____

3. Age
   - ○ 18-30
   - ○ 31-40
   - ○ 41-50
   - ○ 50 above

4. Gender
   - ○ Female
   - ○ Male
   - ○ Prefer not to say

5. Educational Qualification
   - ○ Graduate
   - ○ Post Graduate
   - ○ Professional
   - ○ Others

6. Employment status
   - ○ Business
   - ○ Salaried
   - ○ Student
   - ○ Other

7. Monthly Income

   ○ 50,000

   ○ 51,000 - 1 lakh

   ○ 1 lakhs - 1.5 lakhs

   ○ 1.5 lakhs

8. Since how long you have been using Smart Home

   ○ <1

   ○ 1- 6

   ○ > 6

9. Choose the application areas of Smart Home Devices you use

   □ Energy Management

   □ Home Security

   □ Control & monitoring

   □ Health & wellness

   □ Entertainment

10. Select the Smart Gadgets you use?

   □ Surveillance camera

   □ Smart locks

   □ Video Doorbell

   □ Wireless speakers

   □ Smart Air conditioner

   □ Smart TV

   □ Smoke Detector

   □ Robotic Vacuum Cleaner

   □ Smart lighting Controller

   □ Health Fitness Devices

Please indicate the extent to which you agree or disagree with the following statement in relation to Privacy & security of Smart home

Mark only one oval per row

Sr. No.	Questions	1 Strongly Disagree	2 Disagree	3 Neutral	4 Agree	5 Strongly Agree
11	I feel it is necessary to check whether Data is coming only from authenticated devices	①	②	③	④	⑤
12	I feel information generated by smart devices should not be shared or used by 3rd party (i.e. Advertising / Sales)	①	②	③	④	⑤
13	I would not mind if my health data is shared with my caretaker / friends / relatives / research organizations	①	②	③	④	⑤
14	Do you agree that under emergency, it is OK to disable security authentications	①	②	③	④	⑤
15	if given a choice, would you say YES to government agencies to collect / use my information generated through smart home	①	②	③	④	⑤

16	It is OK to allow government agencies to give access in case of casualties (Fire - brigade)	①	②	③	④	⑤
17	I would prefer to allow Law enforcement agencies to access my data for crime investigation?	①	②	③	④	⑤
18	Do you believe there is a need to offer separate role based management and operational authentication for guests	①	②	③	④	⑤
19	Do you feel your Wi-Fi / Bluetooth should be configured to high level of security?	①	②	③	④	⑤
20	I don’t feel safe storing personal / Family confidential information on smart home system	①	②	③	④	⑤
21	I think privacy is violated when one can’t control how much information is collected by smart devices (e.g. possible storage of all conversations on Alexa / Google	①	②	③	④	⑤

	Assistant)					
22	I believe “Data stored in Encrypted” form will not be altered/Modified	①	②	③	④	⑤
23	I think “Device verification” is necessary to ensure Reliability of data source.	①	②	③	④	⑤
24	I feel, loss of sensitive information can causes harmful Damages like Reputational loss	①	②	③	④	⑤
25	Do you feel necessity to keep Devices at secure (not easily approachable) place to prevent device theft / Damage?	①	②	③	④	⑤
26	I feel worried about unresponsive Security devices	①	②	③	④	⑤
27	Is ease-of- use preferred over security considerations?	①	②	③	④	⑤
28	Do you think Security measures reduces under- friendliness	①	②	③	④	⑤
29	Is cost of automation (Smart devices and related services)	①	②	③	④	⑤

	more important than security considerations					
30	Do you feel system access should be reviewed from time to time (like password updates, security updates from manufacturer	①	②	③	④	⑤
31	Do you think you should get a real-time notification in case of device mal-function?	①	②	③	④	⑤
32	I Expect system should send alerts in case of data modification / alteration	①	②	③	④	⑤
33	Do you think you should get a real-time warning if an anomaly in the home environment is detected?	①	②	③	④	⑤
34	I don’t feel comfortable doing online /financial transactions due to security purpose (e.g. hacking of Wi-Fi)	①	②	③	④	⑤
35	I prefer branded manufactured	①	②	③	④	⑤

	products over local manufacturers					
36	I hope that I can ensure my privacy and Security by living in a Smart Home environment	①	②	③	④	⑤
37	I think it is essential for companies which develop Smart devices should have built in security features	①	②	③	④	⑤
38	Do you feel there should be strict laws to protect Individual Privacy	①	②	③	④	⑤
39	I think Home safety & security is main concern for implementation of smart home technology	①	②	③	④	⑤
40	40. I believe losses, incurred due to information leak can lead to unthinkable damages	①	②	③	④	⑤
41	I Consider Identity theft is the greatest risk against privacy? (e.g. misused in criminal activities)	①	②	③	④	⑤

42	I feel violation of user privacy may result into financial losses.	①	②	③	④	⑤
43	I feel it is necessary to avoid public Wi-Fi for remote access to home system	①	②	③	④	⑤
44	Do you agree that Unauthorized access to System, virus / Worm Attacks Denial of Services are most critical security threats to your Smart home system	①	②	③	④	⑤
45	Do you agree that "Raising consumer awareness regarding security of connected devices" is essential for protecting smart home system	①	②	③	④	⑤
46	I strongly feel Careless or negligent end - users are as dangerous as hackers	①	②	③	④	⑤
47	Do you agree that user should understand the underlying technology to protect from potential hacking / data theft?	①	②	③	④	⑤