ROLE OF DATA ANALYTICS IN SECURITY OF SMART HOMES

Supriya Nagarkar Research Scholar, T.M.V., Pune
Minal D. Kalamkar Research Scholar T.M.V., Pune
supriyanagarkar@gmail.com ; minaldk@gmail.com

Abstract:
A smart home is new trend in architecture in smart cities applications. Smart home data analytics is establishing a preventive care in data processing for identifiable users with a framework for maintaining security & preserving privacy. The research is aimed for role of data analytics in secure data transfer of smart homes. The study includes applications of smart homes and relative networks for analysis of sensor data from smart homes. It includes multiple objectives of smart home data analysis and processing of a big data with potential of the applicability of IoT techniques to provide profitable services. The researcher aims to develop approach of security of system generated and transferred data to control appliances and devices in smart homes. The study is performed for highlighting the needs for Smart Homes in various areas and their future advancements with benefits and implementations. The data analytics play an important role in handling and processing the real-time and continuous data through devices like pc connected to internet and android systems.

Keywords: Data analytics, Data security, Internet of things (IoT), Smart homes, Privacy, Home automation.

Introduction:

In recent years, vast advancement in Internet of Things (IoT) technologies has led to an interesting concept of transforming the home into Smart Home. Data analytics utilizes IoT systems to control all smart automated devices in Smart Home. The roles of data analytics have major involvement in analyzing the data to interpret the needs and technology with various computational methods. The study highlights the key role of data analytics in world of automation of smart homes in terms of utilizing the technology of Artificial Intelligence (AI), multi-agent systems and automation control. Various computational methods for the advancement and development of sophisticated control systems like smart air-conditioners, security devices, mobile phones and home theatres in Smart Home Environment put theoretical smart home into practice.

Smart Home Automation

The smart home based on data analytics is one of the most well-known IoT applications. Home network is connected with heterogeneous devices and controlled remotely through the Internet using embedded sensors ranging from smart speakers to electronic door locks that collect and exchange data seamlessly. The merging of physical and digital worlds inside the home with these technologies is linked to a variety of benefits like improved convenience, energy efficiency, enhanced security and safety [1].

A smart home termed as ‘Domotics’ is a building automation by the remote monitoring and control usingWi-Fi. It also includes an automation of lighting, heating controlled via the Internet that is an important constituent of the Internet of Things [2]

Smart home technologies networked sensors, monitors, interfaces, appliances and devices together and enablelocalised and remote controlled automation of the domestic environment. These controllable appliances and devices likeheating and hot water systems, windows, curtains, garage doors, fridges, TVs,air conditioning and washing machines are connected to sensors and monitors that detecttemperature, light, motion, and humidity and other factors. The software on computing devices or dedicated hardware interfaces are used to control functionality. The devices like smartphones, tablets, laptops, PCs or wall-mounted controls arewirelessly networked, using standardised communication protocols that promote smartness of the smart home [3].

Data Analytics in Smart Homes:

Data analytic technologies are used as assistive services for sensorcollecteddatato effectively perform knowledge discovery algorithms that are implemented in the Safer Home through popular storage solutions and large datasets processing likeHadoop [4].

According to recent study, many communities are currently deploying the future living theme of smart homes as a part of modernization worldwide. The study revealed that data generated through these always-on houses is a real-time and off-line massive amount of valuable data. However, the ability to analysehas significant impact on our society's safety, health, and economy.Smart devices connected to an IoT system can be utilized in health care system fordetecting thestatus of patientsthrough routine or abnormal activities indicating any signs of health problems[5].

The security in the smart home system is used to make accurate decisions that ensure the security, safety, as well as comfort of the residents and their surroundings. Consequently, the studies have explored themultiple systems based on artificial intelligence used for ambient-assisted living and decision support systems combined in smart living environments [6].

The current automated decisions in smart home are based on a rules-engineguided by a set of rules usually defined in a computational elementwith the information received from the sensors databy the user. However, these decision rules based on the external factorsdo not workdue to the changing external environment. The present detection in smart homes is based on motion sensor data [7].

It is observed in the last few years, smart homes concepts have been applied to smart systems in healthcare, energy, security and emergency management, and comfort and entertainment areas. For instance, rehabilitation after acute and chronic diseases is crucial for the quality of the medical outcome, while non-compliance can lead to readmission to the hospital. Therefore it requires medical supervisionto avoid severe health risks.The monitoring systems and technologies with possibilities to transfer into rehabilitationfor closely monitoring the patient to identify risks at home have to be developed [8].

Research Review:

Smart Home Data Analytics

According to the study, data analytics system is based on Data Collector, Data Receiver and Result Provider. A Data Collector is an application at smart home responsible for collecting sensor data that is transferred to the data cluster at regular intervals. The study explains role of Data Receiver module that accepts inputs from the data collectorsperforming an algorithmic function. The requirement of standard process for classification for specific to data processing should be focused on in the study. However, the results from data processing made available to appropriate users to realize the benefits of such a system in healthcare providers, social institutions, service providers and the researchers may all contribute in different ways at improving lives of elderly[9].

Data security in Smart Homes

The researcher has been studied smart homes and some studies explains the use of Internet of Things or IoT and data analytics related to the security of smart homes.It is sensitive ownership issue in healthcare providers or service providers. In terms of data security there is need to know the types of data collection, storage and sharing. However, providers can own the sensor and network devices, yet residents of the homes can pertain the data and stop the collection or destruction of any stored records.The study on data technology includes the sensitive data and preserving it against a malicious user. Many smart homes are secured with Cryptography or VPN techniques for data transfer. Thus, it is important to protect privacy by replacing any personally identifiable information with randomized placeholders, and introducing noise or swapping values. Data is analysed without information loss and transformed with privacy [10].

Smart homes are widely accepted with the fast deployment across the world, becoming a compelling business opportunity for various industrial applications. These smart homes are supported by IoT paradigm and generate large useful data, unlocking the potential of this information. It requires the development of cost-effective and sophisticated big data analytics tools withprocessing, analyzing and managing platforms. Many smart city applications requiretomeet timing requirements of continuous mining of IoT data in sensitive healthcare applications, automatic demand response, safety and surveillance operations. Mostly, these functionalities need predictable latency for near real-time detection and notification and processing data and invoking services from the back-end cloud can face serious constraints. The proximity of resources overcome the high-latency associated with the provisioning of cloud-based services and coordinate the tasks among fog computing nodes, appropriately allocating them from the cloud system[11].

For security of data for smart homes in data analytics, the data access should be ensured through proper authentication and authorization. However, the system should be configurable while assigning rights to execute analysis/mining jobs to appropriate users and access the generated results. Although several methods are used, the role base access control (RBAC) has been usually accepted for its simplicity, flexibility in capturing dynamic requirements that supports for the principle of least privilege and effective privilege management [12].

The study proposes various sensors used in smart homes for various purpose that includes, for example,temperature sensor, water level and gas sensors which are interfaced and controlled by the controller. The role of sensors is important in data analytics. Temperature sensor accurately senses room temperature; gas sensor detects the gas leakage in home, while level sensor measures the water level with specified range. These results are then indicated to personal computer, further sent to the IoT controller and next to the server well secured and safe from the hackers [13].

The data processing results are replaced with these values to avoid information loss for analysis algorithms and preserve privacy. In health areas, doctorscananalyse the current health patterns or can be notified of any anomalies. Theseprovided results must be identifiable for correct care to right patients. The study raised the need for researchers or social institutions to understand the overall health and lifestyle patterns of elderly in a region to improvise results.It also focuses onguaranty the privacy of the data owners'information provided whilethe access control module ensures the right end-users are authenticated and authorized to access data for the requested patient(s). Depending on the role of user, it should make sure the results provided are generalized or suppressed [14].

Methodology:

The researcher aimed to study the application of smart homes technologies and their issues encountered during applications. The data collected during analyzing process have a critical issue of security and privacy at user end that should not arise as threats. The aim of studying data analytics is to put benefits and drawbacks in terms of technologies, processing and the design components of the system to validate the platform and present meaningful results. The researcher has studied several smart home technologies available with secure applications in terms of clarifying the benefit and practicality of the proposed platform [15].

The researcher also found the various applications of smart home technology and the major role of data analytics in security of smart homes. The study discusses various other smart home applications for various fields and proposes a non-intrusive approach for personalised smart home automationwhile integrating and collecting data from open standard IoT devices that uses big data analytics and machine learning. An open-source frameworkslike Apache Spark, Apache NiFi and FB-Prophet are used along with popular vendor tech-stacks, including Azure and DataBricks [16]. The study is based on several researches on use of data analytics and technologies in terms of data security and security of smart homes. Therefore, the researcher used analysis, applications and processes available in different studies to highlight the need for smart homes for security and relation of data analytics for efficient outcomes.

Findings:

Smart Home technologies:

The researcher found that the private sector also realizes the potential of smart homes and relevant new technologies and products are introduced with Smart Things hub to monitor and control electrical devices. While touch point is all-in-one Smart Home Console for light switch indifferent light modes, including bedtime mode, dimming mode by Nybryte app control on different Android and iPhone. A wide-angle camera receives immediate alert for intruders, update weather information, calendar, events and energy monitoring. Such a smart devices include products to control other smart products and also send reminder to the users.

The further enhancement to Smart Home Environments exhibits various forms of artificial intelligence by cultivating traditional home automation systems with online version for smart functions. It increases comfortableness with less operation costs and enhanced security. A myriad of the computational methods used for the design and development of the sophisticated control systems include automation, artificial intelligence (AI) and multi-agent systems.The current trend in smart home system is integration of affordable service robots equipped with artificial intelligence that can respond to voice recognition for human's needs. Zenbo connects to smart home devices withfree and independentmovement around home. It is able to see things through camera, make video calls, recognize faces, and also take photos and videos. These robots control smart things and viewed as a buddy interacting with human. These three generation smart home changes are applicable in several areas [17].

The researcher found that during the past decade, IoT devices have provided smart applications range with state-of-the-art. The smart urban management uses smart transportation management devices, smart electrical and home devices, smart healthcare devices, and many others. The study highlights the aim of one of the most inspiring applications called smart homes for supporting contemporary human living needs. However, security and safety of smart homes are the major concerns challengingthe researchers. Embedding security in theseIoT-based applications is an opportunity to realize the vision of energy-efficient smart homes and buildings. Furthermore, these results inform the community about important recent research trends in smart homes, for formulating future research options[18].

Data Analytics:

Data analytics proposed for secure data transfer in Smart home is studied and the architecture for the secure data collection framework is found suitable for efficient data management.According to this model, three modules like data collector, data receiver and result provider with two storage units. Data collector at smart home transfers sensor data to a data cluster at regular intervals. Data receiver receives the collected data from data collector and transforms them into two different datasets. The storage unit, de-identified sensor data stores the hashed and actual data in identifier dictionary storage for each unique set of quasi-identifiers. The result providercontrols and authorizes end users access to data processing results and privacy of shared results.

Data Analytics Networks:

According to the study, the data transfers should be fast, automatic, secure as well as confidential. The researcher found that it uses cryptographic authentication and automatic session encryption, with integrity protection for transferring the data that is easy to install, use, configure and administer.The speed over wide area networks for bulk data transfer may be affected due to the need of collecting real-time data and frequent rate of transfer, but the size of data per transfer remains small. It is also found that data collector evaluates additional extensions to ensure a secure and high-speed transfer. The result provider module access control modules, to authenticate, authorize and also determine privacy for any data share.

Data Access:

The access control providing access to the system authorizes an end-user and also maintains a privacy level for the shared data. While role based access control is laying out high-level organizational rules and constraints. The identifier retriever prepares a dataset for algorithms to be performed and transformer module guarantee the privacy of shared data. However, it still needs to evaluate the proper approach and practicality. The result processer is swapping the hashed results values from a data processing on the de-identified storage executed for all hashed identifier values.

The resulting hashed identifiers are replaced to ensure the privacy of any shared data is preserved [19].

Security of Smart Homes:

It is found that smart homes are the source of data at IoT gateway from different sources, including household appliances and smart devices. The data acquisition is typically performed by machine-to-machine IoT protocols to communicate with smart home devices and IoT gateways. An IoT gateway mediates between the smart home and the cloud system to provide local processing and storage functions like controlling and filtering of data streams. According to the research, increased use of data analytics offers several advantages to serve multiple households ensuring trusted connectivity and security with enforcement of policy-based access mechanisms. The communication process of data on cloud storage devices is performed with filtering and cleaning, clustering and aggregation in extensive time depending on the nature of the data.Applications of the data acquired may include any activity like recognition to identify health problems, energy consumption patterns and energy saving planning. Generally, it is found effective for individual house owners for using appliances in specific time limit facilitating various energy management programs at home[20].

The study explains the use of non-intrusive sensors such as motion sensors, fire alarms and smoke sensors, door contact sensors, temperature and humidity sensors, pressure sensors for security of smart homes. These sensors are usually deployed and accepted in a smart home environment due to not being intrusive of user privacy and used without capturing activity using video or voice data formats. A user within a smart home is identifiedand the personalisation profiling component automatically controls the home environment intelligently. The recent advancements in the scalable computations and storage facilities of the cloud and big data processing techniques include state-of-the-art IoT capabilities of smartness or intelligencewith better optimal, personalised, long term and balanced intelligent decision in a smart home environment [21].

Conclusion:

The results of the study are not limited to smart homes technologies but also includes various trends in architecture of smart homes. The study has discussed various applications of the smart homes in energy consumption, healthcare systems. The data generated during data analytics process is secured and safe. The advancements of technology have led to opportunity of using internet with end user authentication and remote access to smart home devices.

The Smart home is vastly increasing trend for controlling home devices like fridge, air conditioners, water control or heat control systems, and control of various electrical devices for their uses. In healthcare systems, patients can be monitored for any abnormalities remotely. Therefore, we can conclude the use of smart homes in other sectors with service providers and remote data access.

However, the security of the data used is the major concern to be considered for further implementation to protect from threats. The use of proper security measures and protocols for identifying end user can increase the security of data. It can also be handled using non-intrusive sensors in place of recording of activities with camera or audio devices.

References:

1. Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson, (2021), PRASH:‘A Framework for Privacy Risk Analysis of Smart Homes’,doi: 10.3390/s21196399
2. A.Rajasekar1, J.Samyuktha2 , S. Meharaj3, (2018), ‘Applicability of Big Data Techniques to Smart Home Volume 8 Issue No.3
3. Charlie Wilson, Tom Hargreaves, Richard Hauxwell-Baldwin, (April 2017),‘Benefits and risks of smart home technologies Energy Policy Volume 103, https://doi.org/10.1016/j.enpol.2016.12.047
4. Antorweep Chakravorty, Tomasz Wlodarczyk, Chunming Rong,(2013), IEEE Security and Privacy Workshops Privacy Preserving Data Analytics for Smart Homes, DOI 10.1109/SPW.2013.22

5. Abdul salam Yassinea , Shailendra Singh b , M. Shamim Hossainc , Ghulam Muhammadd, (September 2018),'IoT Big Data Analytics for Smart Homes with Fog and Cloud Computing, Future Generation Computer Systems' 91(4) Project: Smart Meters Big Data, DOI:10.1016/j.future.2018.08.040
6. Habib Ullah Khan, Mohammad Kamel Alomari, &et. Al., (2021), Systematic Analysis of Safety and Security Risks in Smart Homes, CMC, vol.68, no.1, DOI:10.32604/cmc.2021.016058
7. Asaithambi, S.P.R.; Venkatraman, S.; Venkatraman, R., (2021), Big Data and Personalisation for Non-Intrusive Smart Home Automation: Big Data Cogn. Comput. 2021, 5, 6. https://doi.org/ 10.3390/bdcc5010006
8. Andreas Hamper, Isabella Eigner, Nilmini Wickrama singhe, Freimut Bodendorf,(January 2017), Rehabilitation Risk Management: Enabling Data Analytics with Quantified Self and Smart Home Data, Studies in Health Technology and Informatics 236:152-160
9. Antorweep Chakravorty, Tomasz Wlodarczyk, ChunmingRong,(2013), Privacy Preserving Data Analytics for Smart Homes, IEEE Security and Privacy Workshops, DOI 10.1109/SPW.2013.22
10. Antorweep Chakravorty, Tomasz Wlodarczyk, ChunmingRong,(2013) IEEE Security and Privacy Workshops Privacy Preserving Data Analytics for Smart Homes, DOI 10.1109/SPW.2013.22
11. Abdulsalam Yassinea , Shailendra Singhb , M. Shamim Hossainc , Ghulam Muhammadd, (September2018), IoT Big Data Analytics for Smart Homes with Fog and Cloud Computing, Future Generation Computer Systems 91(4) Project: Smart Meters Big Data, DOI:10.1016/j.future.2018.08.040
12. Antorweep Chakravorty, Tomasz Wlodarczyk, Chunming Rong, (2013), IEEE Security and Privacy Workshops Privacy Preserving Data Analytics for Smart Homes, DOI 10.1109/SPW.2013.22
13. A.Rajasekar, J..Samyuktha, S. Meharaj, (2018), Applicability of Big Data Techniques to Smart Home Volume 8 Issue No.3
14. AntorweepChakravorty, Tomasz Wlodarczyk, ChunmingRong,(2013), IEEE Security and Privacy Workshops Privacy Preserving Data Analytics for Smart Homes, DOI 10.1109/SPW.2013.22
15. Antorweep Chakravorty, Tomasz Wlodarczyk, ChunmingRong,(2013) IEEE Security and Privacy Workshops Privacy Preserving Data Analytics for Smart Homes, DOI 10.1109/SPW.2013.22
16. Asaithambi, S.P.R.; Venkatraman, S.; Venkatraman, R., (2021), Big Data and Personalisation for Non-Intrusive Smart Home Automation: Big Data Cogn. Compute. 5, 6. https://doi.org/ 10.3390/bdcc5010006
17. Rita Yi Man Li, HerruChing Yu Li, Cho Kei Mak1 and Tony Beiqi Tang, (2016),Sustainable Smart Home and Home Automation: Big Data Analytics Approach, International Journal of Smart Home Vol. 10, No. 8, pp. 177-198, http://dx.doi.org/10.14257/ijsh.2016.10.8.18 September 2016
18. Habib Ullah Khan, Mohammad Kamel Alomari, & et. Al. (2021), Systematic Analysis of Safety and Security Risks in Smart Homes CMC, 2021, vol.68, no.1 DOI:10.32604/cmc.2021.016058
19. Antorweep
20. Chakravorty, Tomasz Wlodarczyk, ChunmingRong,(2013), IEEE Security and Privacy Workshops Privacy Preserving Data Analytics for Smart Homes, DOI 10.1109/SPW.2013.22
21. Abdulsalam Yassinea , Shailendra Singh b , M. ShamimHossainc , GhulamMuhammadd, (September 2018),IoT Big Data Analytics for Smart Homes with Fog and Cloud Computing, Future Generation Computer Systems 91(4) Project: Smart Meters Big Data, DOI:10.1016/j.future.2018.08.040
22. Asaithambi, S.P.R.; Venkatraman, S.; Venkatraman, R., (2021), Big Data and Personalisation for Non-Intrusive Smart Home Automation: Big Data Cogn. Compute. 5, 6. https://doi.org/ 10.3390/bdcc5010006