SECURITY FRAMEWORK FOR IOT: A REVIEW

Minal D. Kalamkar
Research Scholar,T.M.V., Pune
minaldk@gmail.com

ABSTRACT

The word IoT (Internet of Things) has become popular in research areas of researcher & academicians. The world is going through a transition phase i.e. from Internet to IoT where not only people are getting connected but also different devices that are able to communicate can connect to other devices through internet. In short there will be a world of communicating "things". The IoT paradigm consists of smart objects, actuators and sensors that generates the large data & transmit through internet. The heterogeneous nature of IoT paradigm calls many challenges involved in it. This paper starts with introduction of IoT paradigm, some IoT concepts and its typical structure and finally reviews of IoT security models that have been developed to address security issues in IoT.

KEYWORDS: *Internet of Things (IoT), IoT Paradigm, Thing.*

I. INTRODUCTION

In 1999, Kevin Ashton firstly coined the term Internet of Things [7]. But later in 2005, it was formally introduced by International Telecommunication Union [ITU] in ITU report. IoT was "born" sometime between 2008 and 2009 as per estimated by Cisco IBSG (Internet Business Solution Group).[1] Moreover, Cisco IBSG predicts, by 2015, there will be 25 billion devices connected to the Internet and 50 billion by 2020.Although internet has been a steady growth, IoT is said to be real evolution of Internet.

IoT is going to affect our daily lives in many aspects. Rather we can expect improved quality of life when smart things will guide us throughout the day right from smart homes, healthcare, smart transport systems, smart governance, wastage management and what not. IoT defined by the Cluster of European Research Projects (CERP) [2] The Internet of Things allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. Another definition by ITU-T Y.2060 [8] recommendation –the IoT is a global infra-structure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

The objective of this review is to study the IoT challenges from IoT security perspective along with IoT components and its required security framework.

II. COMPONENTS OF IOT

The typical IoT platform consists of "things", mobile applications & cloud. [11] The IoT devices like sensors, RFID will generate & transmit the data that can be accessed by mobile applications for various purposes and which can also be shared and stored on cloud.

In context with IoT, thing is defined by ITU-TY.2060 - an object of the physical

world (physical things) or the information world(virtual things), which is capable of being identified and integrated into communication networks. Whereas device by ITU is piece of equipment with the mandatory capabilities of communication of sensing, actuation, data capture, data storage, & data processing [10].

Following are the components used in IoT: [4]

1) Sensors- these are electronic equipment which detects or measures a physical property and converts it to an electronic representation. It may be active or passive. To work with different types of sensors, devices should also have the capability of multilingual & interoperable.

2) IoT devices- data generated and transmitted by sensors is transformed into logical information by IoT devices.

3) Protocols- collected data in the form of information is communicated using communication protocol like MQTT, COAP. Communication technologies like RFID, NFC, Bluetooth, ZigBee, WiFi and GSM.

4) Device Gateway- Device gateway is a device which collects data. It has significant computing and networking capabilities. It acts as a bridge between IoT devices and Internet. Gateways communicate with IoT devices using communication protocols also translate the information and send it to cloud [9].

5) Routers/Switches –These are the networking devices which partitioned the trusted and untrusted network.

6) Cloud –it acts as a platform for big data storage. Cloud plays a vital role in IoT because of its capabilities of processing power, storage capacity availability & accessibility from anywhere and from any device.

7) Presentation Devices – like smart phones, tablet or desktop computer. These are the devices using which user can interact with the system. It provides a dashboard to view the information collected.

III. SECURITY MODELS IN IOT

IoT consist of constrained devices that have low storage capacity generally in KB & less RAM (13KB approximately) and limited battery life. To resolve this issue the proposed work of this paper [5] came up with dynamically adjustable security method for Wireless Sensor Networks (WSN) that contains Adaptive Security Manager between wireless sensors & gateways that can select required level of security based on the context and inform the resources.

This framework has been tested for smart factory environment that uses WSN and IPV6 over low power wireless personal area network (6LowPan) with IPSec used for reference communication protocol for constrained devices. The frame work consist of Adoptive Security Manager (ASM) & Adoptive Socket (AS).AS receives instruction from ASM which is tightly coupled to service socket used by application to exchange data. ASM is daemon process that has administrative privileges required to create communication channel with the kernel for controlling security protocols.ASM receives the security level updates from Network Security Evaluator (NSE) that performs security analysis. The architecture consists of AS which has Application Interface, Service Socket, Control Socket and Socket Controller. This architecture enables system to serve resource constrained devices. As it uses many distributed instances, a time synchronization protocol is needed. ASM & AS uses authentication & encryption technique to secure from different attacks. It uses C++ along with its libraries STL, Boost, OpenSSL. Along with it, use of

MYSQL and DBMS functionalities used to get information of users, resources and keys of secured link.

This paper [6] proposes a systemic approach to security in IoT exploring the roles of actors & their interactions in it. The paper describes sections like nodes (person, process, technological ecosystem, and intelligent object), tensions (reliability, Identification, safety, privacy, auto immune, trust, and responsibility) and finally a systemic approach for new applications of IoT in transportation, health care, smart environment domain. To the previous research, the proposed work added the new actor called as 'intelligent object' at the centre of the system. The fundamental role is played by first node i.e. 'person'. Human resources define the security rules, audit it and apply it into operational mode, able to analyze context of IoT finally to exploit the technology; in short what is called as security management.

The second node is 'process' should be compliant with security policies. Thus security process needs to fulfill the requirements of standards, strategies, procedures, policies and required security level. Next node is 'technological ecosystem' i.e. technological choices for IoT security. Information security technology can be categorized into security design and configuration, identification and authorization, system architecture, communications protocols, implemented algorithms, access control methods, performance. Finally 'intelligent object' that is active participant in business, information and social processes. Objects in IoT ecosystem are responsible to communicate, cooperate, share and exchange the information, respond to events.

Further this paper discusses the tensions that represent interaction between the nodes. There are seven tensions which connects the different nodes. First is 'identification and authentication' between intelligent object and person. Privacy and security is critical issue in IoT as any object can have multiple identities. Each tension calls the open research issues. In this case, global ID needs to be considered when intelligent object & human interact. Mobility, privacy, anonymity aspects need more research. Next tension is 'Trust' in between intelligent object and technological ecosystem. Due to heterogeneous nature of IoT ecosystem, there has to be trust in between the objects that can be achieved with digital certificates, exchanging the keys. Research issues in this area are decentralized trust and implementation of trust in cloud, development of application based on node trust, topology of object, coverage deployment, target tracking etc. 'Privacy' tension ties the technological ecosystem with the person. It is the major security issue due to ubiquitous nature of IoT environment. Privacy concerned with data collection, data sharing and its management and data security issues. Open research areas include key management, backup and recovery, asymmetric key management.

'Responsibility' ties the intelligent object with the process. It comes into picture while sharing the data across different resources. So responsibility as a part of security policy must be compliant to access rights and privileges. Research challenges in this area includes access controls rules and identity management.

'Autoimmunity' is in self-loop of the intelligent object node that provides artificial immune system solution to detect intrusions. 'Safety' is the tension that ties the person with the process. Safety measures should be taken into account when sudden failure occurs. Research areas include forest fire, physical security of homes and building. 'Reliability' ties the process with the technological ecosystem. The reliability deals with availability of data over the time. Research issues in this area are developing automated solution for IoT service management.

The paper [3] addresses security issues authorization & access control for distributed, cross domain systems containing resource constrained devices that are not directly accessed by human. In fact it focuses on the problem of single constrained device communicating with other domains. It uses main feature of IoT i.e. distributed –centralized approach to take authorization decision based on local conditions. The paper proposes model called smartORBAC (Organization based access control model) using centralized – distributed approach where authorization decision based on context (local condition) aware access control which is applied for typical healthcare scenario.

The previous work (ORBAC Model) didn't fulfill the needs of distributed, collaborative, interoperability needs required for cross domain communication. Hence smartORBAC model came up with collaboration and context aware concepts along with the enhanced architecture that is composed of four functional layers. It has different functional layers and distributes processing cost into constrained devices and less constrained devices while simultaneously addressing collaborative aspect. Further it talks about centralized architecture, distributed approach & centralized - distributed approach based on position of access control. The smartORBAC model has 4 actors viz. RS (resource server) Resource Owner (RO), Client(C) and Client Owner (CO). SmartORBAC architecture based on partitioning of access control process into functional layers like constrained layer in which Resource Server (RS) & Client (C) are located. In less constrained layer Client & resource authorization engine (viz: CAE & RAE, i.e. in charge of the device) resides. The group of constrained actors is connected to less constrained actor belonging to the same security domain. Organizational layer contains ROr & COr represents Resource Organization & Client Organization respectively. The organization decides security policy and authorization policy for the device. Collaboration layer where access rule of given resource are jointly defined.

Before initiating the interaction an agreement is passed between the entities. The principal authorization manager (PAM) manages this agreement. Every organization decides which resources it will allow to access to external partners and reference it into PAM. When request comes for a specific referenced resource then COr and ROr negotiate and pass the agreement about use of R resulting into a contract and security access rule for R. Finally COr and ROr exchange the format.

For implementation of this model, they've used COAP (Constrained Application Protocol) along with JSON (JavaScript Notation) based notation for authorization request & response. JSON is a lightweight data interchange format that reduces size of messages & optimizes processing time.

This paper covers only authorization aspects but didn't focus on authentication process as well as the Client Organization's (COr) and Resource Organization's (ROr) contract and exchange format has not been discussed.

IV. CONCLUSION

After studying the above security framework models, it can be concluded that despite of there is no standardization of IoT security framework, implementation of the security framework should be based on the domain of application (for e.g. healthcare, transportation, infrastructure, industry etc.), type of required devices used in it i.e. constrained or non- constrained.

Depending up on the security levels, dynamically security level can be adjusted using adoptive security framework model as that will serve the issues regarding constrained devices used in Wireless Sensor Networks (WSN).

To ensure safety, it also need to see if decisions are based on real time contextual information, for that, type of access control model need to decide. viz. centralized, distributed or centralized-distributed access control.

To resolve the issues related to clock drift, time synchronization protocols like NTP should be used where the time is critical factor to be considered. Along with that the collaborative aspect should be considered in case of use of interoperability of domains.

REFERENCES

[1] D. Evans, 2011, "The Internet of Things - How the Next Evolution of the Internet is Changing Everything", 'CISCO white Paper', Pg.3, Available at:<http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>

[2] Salim Elbouanani, My Ahmed El Kiram and Omar Achbarou, 2015,"Introduction To The Internet Of Things Security", '8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) IEEE', Pg.33

[3] Imane Bouij-Pasquier, Anas Abou El Kalam, Abdellah Ait Ouahman, and Mina De Montfort, 2015, "A Security Framework for Internet of Things", 'Springer International Publishing Switzerland', Pg.19-31

[4] Mayank Dixit, Jitendra Kumar, Rajesh Kumar, 2015,"Internet of Things and its Challenges", 'International Conference on Green Computing and Internet of Things (ICGCIoT) IEEE',Pg.810

[5] Enrico Ferrera,Rosaria Rossini, Davide Conzon, Claudio Pastrone, Sandro Tassone, 2016, "Adaptive Security Framework for Resource – Constrained Internet –of – Things Platforms", '8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) IEEE', Available at:< http://ieeexplore.ieee.org/document/7792431/>

[6] Arbia Riahi, Yacine Challal,Enrco Natalizio,zied Chtourou, 2013, "A systemic approach for IoT security", 'International Conference on Distributed Computing in Sensor Systems IEEE', Available at:< http://ieeexplore.ieee.org/document/6569455/>

[7] [7]RFID, 2009,"That 'internet of Things' Thing", Available at :<http://www.rfidjournal.com /articles/view?4986>,[Accessed 10 March 2017]

[8] ITU,2012, "Overview of the internet of things", Available at:<https://www.itu.int/rec/T-REC-Y.2060-201206-I>, [Accessed: 10 March 2017]

[9] Prokarma, 2015,"IoT Gateways: The way to IoT Networking",Available at:<https://www.prokarma.com/blog/2015/02/17/iot-gateways-way-iot-networking>,[Accessed:11March2017]

[10] ITU,2012, "Overview of the internet of things",Pg.4 Available at:<https://www.itu.int/rec/T-REC-Y.2060-201206-I>, [Accessed: 10 March 2017]

[11] Salim Elbouanani, My Ahmed El Kiram and Omar Achbarou, 2015," Introduction To The Internet Of Things Security", '8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) IEEE', Pg. 33

CALL FOR PAPERS

At the outset, I take this opportunity to introduce ***"Cyber Times – International Journal of Technology & Management"*** which is a platform to provide an innovative view of Technology, Management thinking, Realistic Research Studies and various Management Practices in the Indian and Global perspective.

The ***"Cyber Times – International Journal of Technology & Management"*** is Bi-Annual Double Blind Peer reviewed International Journal with ISSN: 2278-7518 with both online and print versions. Cyber Times, Call for original research papers for Vol. 10 Issue 2 from the Research Scholars, Academicians, Industry Professionals, Govt. officials to be published till September-2017 edition in different domains of Engineering, Technology, Management, Science and all other categories. Download the latest and detailed Author Guidelines from http://journal.cybertimes.in

Last date of Abstract Submission: 15th August' 2017
Last date of Full Paper Submission: 15th September' 2017 (Without Late Fee)
Last Date of Full Paper Submission: 30th September' 2017 (With Late Fee)

Note:

- The papers received for the final publication will be screened by the Evaluation Committee for approval and only the selected Papers will be published in the coming edition. Further information is available on the website (http://journal.cybertimes.in) under the "Guidelines for paper Submission" section.

You are cordially invited to contribute your Research Paper for the publication in our next edition. Authors are encouraged to submit their Research work document via Email. Abstract, and Full Length Paper should be sent in .doc or .docx as an attachment separately to editor@cybertimes.in

Moreover, in case of any further queries; please feel free to contact us and we'll be happy to assist you in a better way.

Looking for a Long-Term Association

Thanks & Regards,

Dr. ANUP GIRDHAR

Editor-in-Chief (CYBER TIMES)

"SEDULITY SOLUTIONS & TECHNOLOGIES" is an ISO 9001:2008 Certified Organization. It is a channel to provide the best Technical Solutions to various Corporate, Law-Enforcement Agencies, Private/ Govt. Institutions etc. '**Sedulity'** is the most professional group of IT Experts and Ethical Hackers and involved into various Cyber Security Solutions, Secure Development, Open Source Projects, E-Learning, and Cyber Forensics Solutions. We are Equipped with a team of Certified Ethical Hackers, Forensic Experts, Secure Coders and Linux/ Networking experts from across the globe involved in providing End-to-End Cyber Security, Customized IT Solutions and Hi-Tech Corporate Trainings.

Services/ Solutions/ Products Offered are as follows:

- **Penetration Testing/ IT Auditing**
- **Cyber Crime Investigation**
- **Network Architecture Designing & Security**
- **Research & Development**
- **Publications**
- **Cyber Security AMC's via 'Sedulity Operating System' or other Linux & Windows Operating System**
- **Cyber Forensics and Data Recovery**
- **Server Configurations (File Sever, SMS Server, Web Server, Database Server, E-Mail Server, Proxy Server, and many more….)**
- **Hi-Tech Industrial Trainings for Faculties, Students, Corporate & Govt. Professionals**
- **Secure Website/ Web Portal Development**
- **E-Learning Solutions**
- **SEO and many more…**

For More details;

Contact:
Ph: 011-25595729, +91-9312903095
Email: contact@sedulitygroups.com
Website: http://sedulitygroups.com

Industrial Trainings Offered for Corporate, Faculties, students:

- LAMP + CMS
- Cloud Computing
- Advance PHP with CMS
- SEO
- CCNA/ Network Administration
- Linux Administration
- JAVA/ Android Programming
- C, C++, Data Structures
- Embedded Systems
- IoT (Internet of Things)
- Data Mining / Data Analytics
- Personality Development

Learn "Cyber Security & Ethical Hacking" and get Certified from 'IGNOU' or 'TMV-Pune' or 'IETE'

Get Enrolled for:

- Post Graduate Diploma in Information Security (IGNOU)
- Advance Certificate in Information Security (IGNOU)

OR

- Post Graduate Diploma in Cyber Security (TMV)
- Advance Diploma in Cyber Security (TMV)
- Diploma in Cyber Security (TMV)

Contact Details:

For Delhi:

H/O: 310 Suneja Tower-II, District Centre, Janak Puri, New Delhi-110058.
Phone numbers: 011-25595729, +91-9312903095.
Email: contact@sedulitygroups.com, Website: http://sedulitygroups.com

For Pune:

B/O: 568, 2nd Floor, Computer Department, Tilakwada, Narayan Peth, Pune-411030
Phone numbers: +91-9860201117, +91-9312903095.
Email: pune@sedulitygroups.com, Website: www.sedulitygroups.com