Survey On Issues In Authentication Based Iot Security

Dr. S. Kamalakkannan, Ms.N. Sivasankari

Abstract : Internet of Things (IoT) is a network of devices which can sense, accumulate and transfer data over the internet without any human intervention. The IoT is an ever-growing network of devices which connect to each other using various networking standards and protocols. But the infrastructure can be viewed as a hierarchy, where endpoint devices connect to larger networks. These end points may be inherently secure but in case of integration into a system security is an issue. The main objective of this paper is to provide the security related issues in an IoT environment.

Index : IoT, Authentication, Security Mitigation

1 INTRODUCTION

Internet of Things (IoT) is one of the rapidly growing technologies in the field of modern wireless communications. It connects smart objects and devices used in our everyday life to the Internet. It opens the door for new ways of data exchange [1]. IoT introduces the concept of smart world in wide range of applications, like smart cities where it manages parking spaces, street lighting, and irrigation facilities, smart homes which are really safe and more efficient to live, smart environment that can automatically monitoring the pollution from air and water, etc. However, secure communication in IoT raises many serious challenges which need to be addressed carefully for large-scale and commercial deployment of such networks. The purpose of this research paper is to focus on the issues related to authentication based security in IoT. Section II explains the basic architecture of IoT. Section III focuses on the various technical challenges involved in IoT. Section IV explains the security architecture and development of current security mechanism in Section V. The authentication based security and its weakness are depicted in section VI.

2 IOT ARCHITECTURE

IoT is the technology that builds systems capable of autonomously sensing and responding to stimuli from the real world without human intervention. The architecture of an IoT is classified into four stages as shown in fig 1. Stage 1 is the Sensors/Actuators, basic components of an IoT, giving the ability to emit, accept and process signals. The signals received from the sensors/Actuator are in analogue form which needs to be aggregated and converted into digital streams for further processing which is taken care by stage 2 i.e. Data acquisition systems. Data acquisition systems perform these data aggregation and conversion functions. Once IoT data has been digitized and aggregated, it may require further processing before it enters the data center; this is where stage 3 Edge Analytics comes in.

- *Dr.S.Kamalakkannan, Associate Professor, Department of Information Technology, School of Computing sciences, VISTAS (Vels Institute of Science, Technology & Advanced Studies) Chennai, India.. E-mail: Kannan.scs@velsuniv.ac.in*
- *Ms.N. Sivasankari, Research Scholar, Department of Computer Science, VISTAS (Vels Institute of Science, Technology & Advanced Studies) Chennai, India.. E-mail: sivasankari1985.n@gmail.com*

Stage 4 is the cloud analytics, data that needs more in-depth processing gets forwarded to physical data centers or cloud-based systems.

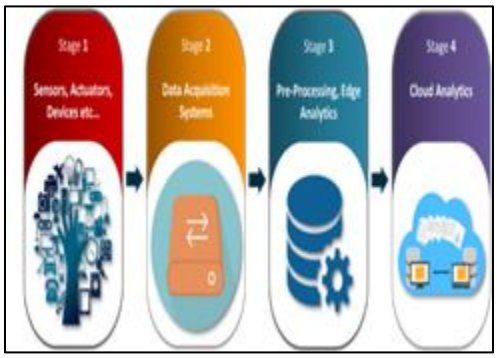

Fig1. *Stages in IoT*

3 TECHNICAL CHALLENGES IN IOT

Eventhough IoT hailed as one of the biggest breakthroughs in the history of the tech industry, it still need proper solutions and approaches for the four basic technical challenges such as security, privacy, compatibility and connectivity [2].

3.1 Security

There are many reasons behind the state of insecurity in IoT. Every vendor is hastily seeking to provide new innovative connected gadget before competitors do. Under such circumstances, they focus mainly on their functionalities, so security takes a back seat. Scalability issues also contribute to the creation of insecure IoT products.

3.2 Privacy

IoT devices also collect sensitive data that is often protected by legislations like Health Insurance Portability and Accountability (HIPAA) in the U.S. However, special precautions needed for handling such information are amiss. Another thing to take into consideration is that while data generated by a single device may not be sensitive, it may reveal a lot of personal information when combined with data from other appliances.

3.3 Connectivity

Connectivity is one of the major challenges in IoT due to connecting large number of devices. In traditional network, client/server model is used to authorize and authenticate the connected nodes but it is not sufficient for connecting IoT

devices due to its increasing growth; it will lead to bottleneck. Moreover, current cloud server capability is also not sufficient to handle large amount of data; it can break down

3.4 Compatibility

Different technologies like ZigBee, Z-Wave, WI-Fi, Bluetooth and, Bluetooth Low Energy (BTLE) are all battling to become the dominant transport mechanism between devices and hubs. This becomes major source of problems when a lot of devices have to be connected; such dense connectivity requires the deployment of extra hardware and software. There are various compatibility issues that are bound to stem due to the non-unified cloud services and lack of standardized M2M protocols. IoT automates every object in our day to day life; it is a system of growing complexity. When compared to big data and cloud, IoT is a new area and it promises a bright future. So, lots of researches are going to find better solutions for the above mentioned challenges as shown in figure 2.

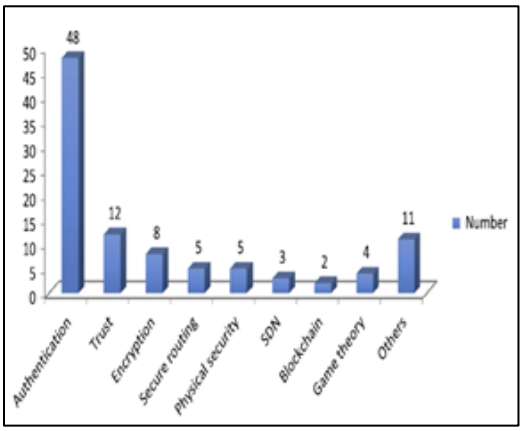

***fig 2**. Challenges in IoT*

4 IOT SECURITY

IoT security is an area which is important in order to safeguard the system and the hardware; it is more challenging because of its heterogeneity nature and scalability (i.e) increasing in the number of nodes in the system. The current security measures which are applied in a conventional network may not be sufficient for IoT environment.IoT can be viewed as a three layered architecture: Perception/hardware layer, a Network/communication layer, and a layer of interfaces/service [3]. The basic building blocks that make up an IoT system are hardware/devices, communication/messaging protocols, and interfaces/services. According to Open Web Application Security Project (OWASP), attack vectors concern all the three layers of an IoT system. So, the implemention of IoT security should encompasses all the three layer of IoT as presented in Fig 4.By referring the architecture of IoT, security issues are pertinent at all three IoT layers. Securing IoT systems presents a number of unique challenges, such as unreliable communications, hostile environments, and in-adequate protection of data and privileges [4].

5 DEVELOPMENT OF CURRENT IOT SECURITY MECHANISM

IoT is an interconnection of people, devices and the internet. So, the system should ensure privacy, confidentiality and availability. To preserve security and guarantee the availability of the services offered, IoT system should encompasses security mitigation. So, applying security mitigation is the main objective of IoT developers. Thus, the mitigation and countermeasures are usually applied according to the classic threat vectors. Fig. 3 shows the trends in the techniques and methods which have been used in 2016–2018. From the figure it is observed that authentication is still the most popular technique for security. Trust management is gaining popularity, due to its ability to prevent or malicious node. Also, the research on encryption is focusing on lightweight and low-cost encryption for low-power and constrained devices. New technologies such as SDN and blockchain are focusing on distributed environment.

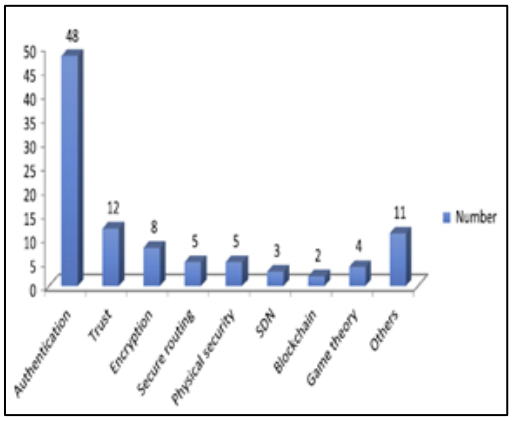

***Fig 3.** publications in IoT security from 2016 to 2018*

5 AUTHENTICATION MECHANISMS

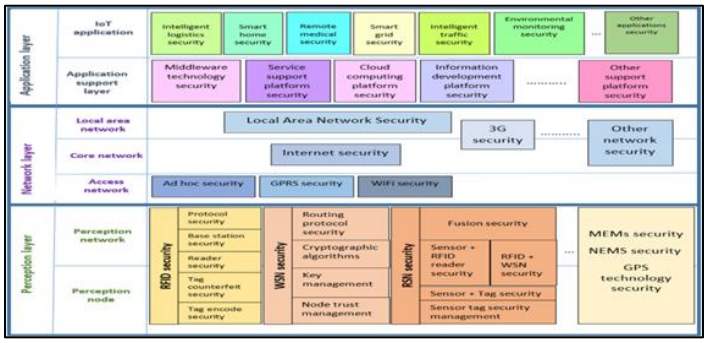

***Fig 4.** IoT Security Architecture*

Authentication is the process of identifying users and devices in a network and granting access to authorized persons and non- manipulated devices. Due to inadequate procedures in authentication and authorization, the hackers can gain easy access to IoT devices. Currently the protocols that supports authentication are MQTT, DDS, Zigbee and Zwave. Even developers are focusing and providing tools required for authentication in IoT communications, messaging and pairing, but still the communication in IoT devices are hijacked. Further, insecurity in network services, allow bad actor or the threat to explore the network and propagate through it. In network layer, authentication is the currently most popular

and using security method to achieve secure communication. Researches ongoing in authentication are discussed in the next section.

6.1 IoT authentication methods

Applying authentication security mechanism in IoT system faces several challenges due to heterogeneous protocols used in IoT system, its scalability nature, supporting different communication channels, and constrained in multi-vendor devices. The challenges faced by authentication security are mentioned briefly in this section.

1. The Key Agreement (LKA) protocol is proposed by [5]. It is based on the Internet Key Exchange (IKEV2) and designed to provide end-to-end security between IPv6 and 6LoWPAN nodes. But, it is only applicable to IP based devices, which need to be equipped with the relevant authentication tools.
2. Lightweight and privacy-preserving mutual authentications are proposed by [6]. It includes lightweight cryptographic functions but it should be synchronized with cloud server and does not support dynamicity.
3. A secure and efficient user authentication scheme for multi-gateway wireless sensor networks is proposed by [7].
4. This scheme supports both dynamicity and scalability but has a higher computational overhead.
5. An enhanced authentication and key establishment scheme is designed for M2M communications in the 6LoWPAN networks (EAKES6Lo) [8]. This scheme used hybrid cryptography approach and supports both static and mobile nodes in 6LoWPAN networks but it is energy consuming for resources constrained devices.
6. An end-to-end security protocol for 6LoWPAN (6LowPSec) [9] is proposed to perform security functions only at end devices. It is implemented at the adaptation layer.
7. A two-factor authentication and key agreement scheme in 5G- integrated WSNs for the IoT is proposed in [10]. It supports anonymity attacks in authentication process but it's computational and communication cost is high. So it is not suited for normal sensor nodes.

However, all the proposed authentications still have some limitations and the use of a public key for lightweight authentication is still not the ultimate solution for security mitigation since a public key can be stolen [11]. Moreover, authentication may be bypassed by some malicious codes or statements. In [12] and [13] the weaknesses of the current solutions for IoT authentication are elaborated as listed below:

- Taken verifier assault and many signed in clients with the equivalent login ID assault.
- Denial-of-service attack and node capture attack.
- Replay attack and forgery attack.
- Stolen smart-card and sensor-node impersonation.
- Gateway node bypassing and sensor-node key impersonation.
- Off-line password guessing attack, off-line identity guessing at- tack, smart card theft attack, user impersonation attack, sensor node impersonation attack.

7 CONCLUSIONS

This paper focused on the various key areas where research has to be made for successful implementation of IoT devices which is going to be the future world. It briefly explained about authentication based challenges such as Key Agreement Protocol, lightweight cryptographic functions, multi-gateway WSN, an enhanced authentication based key establishment scheme, a two-factor authentication, and key agreement scheme in 5G- integrated WSNs.

8 REFERENCES

[1] Mangal Sain, Young Jin Kang, Hoon Jae Lee, Survey on Security in Internet of things: state of the art and challenges, ISBN 978-89-968650-9-4

[2] Website https://www.allerin.com/blog/4-challenges-that-are-faced-by-iot-developers

[3] Mardiana binti Mohamad Noor, Wan Haslina Hassan, Current research on Internet of Things (IoT) security: A survey 1389-1286/© 2018 Elsevier B.V. All rights reserved.

[4] K. Chen , S. Zhang , Z. Li , Y. Zhang , Q. Deng , S. Ray , Y. Jin , Internet-of-Things Security and Vulnerabilities : Taxonomy, Challenges, and Practice, Journal of Hardware and Systems Security 2 (2018) 97–110 .

[5] M. Lavanya , V. Natarajan , Lightweight key agreement protocol for IoT based on IKEv2, Comput. Electr. Eng. 64 (2017) 1339–1351 .

[6] F. Wu , X. Li , L. Xu , S. Kumari , M. Karuppiah , J. Shen , A lightweight and priva- cy-preserving mutual authentication scheme for wearable devices assisted by cloud server, Comput. Electr. Eng. 63 (2017) 168–181 .

[7] J. Srinivas , S. Mukhopadhyay , D. Mishra , Secure and efficient user authentica- tion scheme for multi-gateway wireless sensor networks, Ad Hoc Networks 54 (2017) 147–169 .

[8] Y. Qiu , M. Ma , A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks, IEEE Trans. Ind. Informatics 12 (6) (2016) 2074–2085 .

[9] G. Glissa , A. Meddeb ,6LowPSec: An End-to-End Security Protocol for 6LoW- PAN, Ad Hoc Networks 82 (2018) 100–112 .

[10] S. Shin , T. Kwon , Two-factor authenticated key agreement supporting un- linkability in 5G-integrated wireless sensor networks, IEEE Access 6 (2018) 11229–11241 .

[11] V.S. Latha Tamilselvan , Prevention of blackhole attack in MANET, The 2nd In- ternational Conference on Wireless Broadband and Ultra Wideband Communi- cations (AusWireless 2007), 2007 .

[12] M. Lavanya , V. Natarajan , Lightweight key agreement protocol for IoT based on IKEv2, Comput. Electr. Eng. 64 (2017) 1339–1351

[13] T. Shinzaki , I. Morikawa , Y. Yamaoka , Y. Sakemi , IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data, Fujitsu Sci. Tech. J. 52 (4) (2016) 52–60