IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

A Review Paper of Security in Internet of Things (IoT)

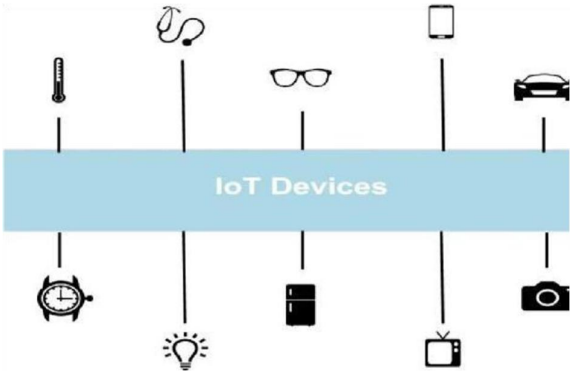
Akshitha C V[1], Apoorva Hosamani[2], Soundarya S Siddanagoudra[3], Vasudev Shahapur[4]
Students, Department of Computer Science and Engineering[1,2,3]
Assistant Professor, Department of Computer Science and Engineering[4]
Alva's Institute of Engineering and Technology, Mangalore, India

Abstract: *Internet of Things (IoT) has drawn important attention in recent years since it has made revolutionary changes in human life. The IoT enables the exchange of information or data in a wide variety of applications such as smart buildings, smart health, smart transport, and so on. As billions of connected things communicate with each other and can interchange sensitive information that may be revealed. Hence, strengthening IoT's security and preserving users' privacy is a crucial challenge. The aim of this paper is to provide a comprehensive study of the IoT security. Several IoT security attacks are examined and a taxonomy of the security requirements based on the attacks purposes is proposed. Furthermore, recent security solutions are described and classified based on their application area. Ultimately, open research directions and security challenges are discussed.*

Keywords: Internet of things (IOT), wireless sensor, security, privacy, issues networks.

I. INTRODUCTION

The conception of the Internet of Things has been introduced by Kevin Ashton in 1999. IoT aims to link anything at anytime in anyplace [1]. Things in the IoT include physical objects from tiny to very large machines that ideally communicate with each other via the Internet without human intervention [2]. The IoT devices are provided with sensors to capture data and actuators to autonomously and intelligently perform actions [3]. Over the past few years, the IoT has gained significant attention since it brings potentially enormous benefits to the human. The primary objective of the IoT is merging of these numerous diverse application domains under the same umbrella referred as smart life [4]. Shortly, billions of devices expected to be linked to the Internet [5]. Hence, an increasingly huge amount of data will flow within the Internet [6]. This data can face several security attacks such as eavesdropping and altering. Consequently, the user's privacy will be threatened [7].



Wireless Sensor Network (WSN) consists of a huge number of physical autonomous sensors deployed in the environment in order to control the environmental conditions [1]. The WSNs are prone to different type of attacks such as sinkhole and wormhole attack, node tampering and jamming, etc [6].

Radio Frequency Identification (RFID) is used to recognize and track IoT objects. It allows data interchange via radio signals

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

over a short distance [1]. Similar to the WSN, the RFID technology has many vulnerabilities including spoofing, cloning, and sniffing [6].

Cloud computing plays major role in the IoT by offering an unlimited storage resources and processing power [10]. Constrained Application Protocol (CoAP) is an application layer protocol used for resource-constrained devices [11,12].

IPv6 Low power Wireless Personal Area

Network (6LoWPAN) joins IPv6 and LoWPAN and allows transmission of IPv6 packets above IEEE 802.15.4 networks [11]. The 6LoWPAN is worthy for the IoT and has several advantages. However, it is receptive to various attacks like DoS (Denial of Service) and eavesdroping attacks [13].

Ultra-Wide Band (UWB) is a practicable technology for a wide variety of IoT applications due to its low power consumption, higher precision, and security [14]. IEEE 802.15.4 is a protocol to the physical layer and the MAC (Medium Access Control) layer in Wireless Personal Area Networks (WPANs). It provides the link of things in personal area with low energy consumption [11].

Near Field Communication is a short-range technology that can be used in several IoT systems such as payments and authentication. The NFC issues easy network access and data exchange. However, it is susceptible to information leakage since the wireless signal created by device can be picked up by an attacker [15,16].

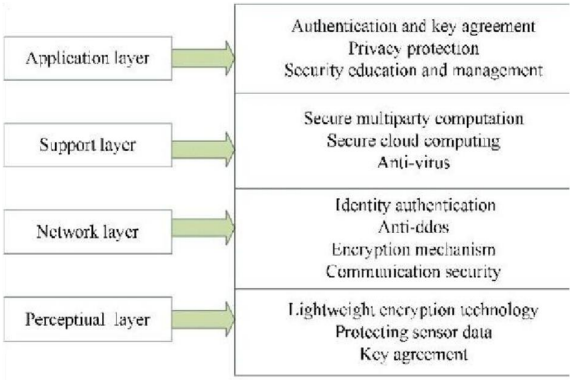
In this stage, the ambient intelligence and autonomous control are not a chunk of the original concept of IoT. With the growth of advanced network techniques, cloud computing, there is a shift integrating the concepts of IoT and autonomous control in M2M research to build an advancement of M2M in the form of CPS. Therefore, some new methodologies and technologies should be developed to meet the higher requirements in terms of security, reliability, and privacy [3].

II. SECURITY

If one thing can prevent the Internet of things from changing the way we live and work, it will be a breakdown in security. While security considerations are not new in the factor of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a basic priority. Users need to believe that IoT devices and related data services are fixed from vulnerabilities, mainly as this technology become more pervasive and integrated into our daily lives. Main challenge is the integration of security mechanisms and the user acceptance. User must feel that they control any data that is related to them rather than they feel they are being controlled by the system. This integration causes new requirements, not been previously considered.

2.1 Secure Architecture

IoT are divided into four key levels [7]. Figure. 1 shows the level of architecture of the IoT.



The most basic level is the perceptual layer (recognition layer), which collects all kinds of data through physical equipment and identifies the physical world, the data includes object properties, environmental state etc and physical equipments include RFID reader, all types of sensors. Second level is network layer. Network layer is responsible for the dependable transmission of data from perceptual layer, initially processing of information, classification and polymerization. The third level is support layer. Support layer will set up a dependable support platform for the application

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

layer, on this support platform all kind of intelligent computing powers will be arranged through network grid and cloud computing. It plays the role of merging application layer upward and network layer downward. The application layer is the topmost level. Application layer gives the personalized services according to the needs of the users. Network security and management play a major role in above each level. Then we will analyse the security features.

2.2 Security Features

- Perceptual level: Perceptual nodes usually have less computer power and storage capacity because they are simple and with less power. Therefore it is unable to apply the frequency communication leap and public key encryption algorithm for security protection. And it is very difficult to configure the security protection system. Meanwhile, external network attacks such as Denial of service also brings new security problems.
- Network layer: although the core the network has relatively complete security protection capabilities, but Man-in-the-Middle attack and counterfeit attack yet meanwhile there
- are junk mail and the computer The virus cannot be ignored, a large number of sending data causes congestion. And therefore, security mechanism at this level is very important to the IoT.
- Support layer: Make bulk data intelligent processing and decision of Network behaviour at this layer, intelligent processing is limited to harmful information, so it is a challenge to improve the ability to recognize the malicious information.
- Application Layer: In this level security needs for various application environment are different, and data sharing is that one of the characteristics of application layer, which creating problems of data privacy, access control and disclosure of data [18,19].

2.3 Security Requirements

According to the above analysis, we can summarize the security requirement.

- Perceptual layer**:** In the first node, authentication is necessary to prevent illegal access to the node; second, to protect the confidentiality of the transmission of information between nodes, data encryption is an absolute necessity. To solve this problem it is important to use lightweight encryption technology. While the integrity and authenticity of sensor data is becoming the focus of research, we'll discuss this issue in more detail in the next section.
- Network layer: In this layer, the existing communication security mechanisms are difficult to be applied. Furthermore, distributed denial of service (DDoS) attack is a common method of attack on the network and is particularly severe in the Internet of Things, so preventing the DDOS attack for the vulnerable node is another problem to be solved at this layer.
- Support layer: Support layer needs a large part of the application security architecture, such as cloud computing and multi-party secure computing, almost all strong encryption algorithm and encryption protocol, technology of stronger system security and antivirus.
- Application layer: To resolve the security problem of the application layer, need two aspects. One is key authentication and agreement across the heterogeneous network, the other is user privacy protection. In addition, education and management are very important for information security, especially password management [18,19].

IOT security and privacy requirements. Security and privacy are crucial enabling technologies. Therefore, it is important for IoT architectures to consider and solve these challenges early. However, the uniqueness of the IoT introduces new scale and manage the heterogeneity of data sources. The related IoT security surveys are nothing with respect to the requirements. To provide a comprehensive overview, we summarize these security requirements from the IoT domain and divide them into five groups: network security, identity management, privacy, trust, and resilience. Furthermore, identity management is affected by the heterogeneity of the IoT. Privacy is primarily related to scalability and limited resources as restrictions are placed on the technology candidates that can be used. Finally, resilience is directly related to the IoT's need for scalability.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

Network Security: Network security needs are splitted into confidentiality, authenticity, integrity and availability. Factors such as heterogeneity and constrained resources must be considered when applying them to IoT architectures. Interconnecting devices requires greater confidentiality.

Privacy: Privacy is considered one of the main challenges in the IoT. Due to the involvement of humans and the increasingly ubiquitous data collection.

e.g. identity of a person. This requirement is considered a great challenge as nearly all other tracking devices collect personal information and a large amount of that data becomes Personally Identifiable Information (PII) when combined together; enough to identify a person. One person not identifiable as a data source or an action is anonymity, another challenge they face in IoT such as mobile devices and wearable sensors that may cause personally identifiable information such as IP addresses and location to be leaked unknowingly. Intel Security also announced that its Enhanced Privacy Identity (EPID) technology will be upgraded to other silicon vendors.

Identity management: Identity management must be given comprehensive attention in the Internet of Things due to the number of devices and the complex relationship between devices, services, owners, and users. Authentication and authorization methods including revocation, accountability or nonrepudiation are required.

Resilience: Robustness and Resilience against attacks and lack of success becomes another major challenge due to the large scale of devices. IoT architectures must provide mechanisms to competently select elements, transmission paths and services according to their robustness (prevention of failures / attacks)

2.4 Requirements for Growing

Applications With the development of WSN, radio frequency identification (RFID), pervasive computing technology, network communication technology, and real-time distributed control theory, CPS, an emerging form of IoT, is becoming a reality.As said above, the security challenges of the Internet of Things are severe. It is essential to establish a sound security structure. Policies and regulations related to the Internet of Things will also be a challenge.

III. CHALLENGES

IoT as a very active and new research field, to solve a variety of questions, in different layers of architecture and from different aspects of information security, the following subsections analyse and summarize common security challenges of IoT.

- **Security Structure:** In[19], the IoT will remain stable and persistent as a whole over time, putting together can security mechanism for each logical layer not implement the defence in depth of system, so it is challenging and important research area to build security structure with the combination of control and information.
- **Keynismo**, is always in fashion investigation area. Lightweight cryptographic algorithm or higher sensor node performance is not yet applied. Network security problems will be pay more attention and become the key points and difficulties of research in this network environment[18,9].
- **Security Law and Regulations:** Currently, security laws and regulations are still. Not the main focus, there is no technology standard around the Internet of Things. The IoT
- is related to national security information, business and personal secrets privacy.

- **Requirements for Burgeoning:** In this system, the high Security is necessary to ensure order performance. The large-scale sensor network is always a challenge, and the policies and regulations related to IoT will also be a
- challenge.

IV. CONCLUSION

The number of IoT devices is increasing and the amount of data is increasing as well. To ensure end-to-end security in the context of IoT, standardized security protocols are highly required. In this paper, we review the latter related business and its shortcomings. This classification can help developers and researchers in the design of new schemes for security address in the context of the IoT. We've also detailed some current safety data. Finally, we conclude that the evolution of IoT faces many security issues. The main challenge is develop effective and adaptive safe mechanisms for limited resources devices.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, March 2022
Impact Factor: 6.252

REFERENCES

[1] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645.

[2] Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120.

[3] Saif, I., Peasley, S., & Perinkolam, A. (2015). Safeguarding the Internet of Things: Being secure, vigilant, and reilient in the connected age. Deloitte Review, 17. https://www2.deloitte.com/insights/us/e n/ deloitte review/issue-17/internet-ofthings-datasecu rity-and-privacy.html. [4] Vermesan, O., & Friess, P. (2013). Internet of Things: Converging technologies for smart environments and integrated ecosystems.

[4] Aalborg: River Publishers.

[5] Singh.S,&Singh,N.(2015). In 2015 International conference on Green computing and Internet of Things.IEEE.

[6] Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of Internet of Things. arXiv preprint arXiv:1501.02211.

[7] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 20(8), 2481.

[8] C. P. Mayer, "Security and privacy challenges in the internet of things," Electronic Communications of the EASST, vol. 17, 2009.

[9] T. Polk, and S. Turner. "Security challenges for the internet of things," http://www.iab.org/wpcontent/IABuploads /2011/03/Turner.pdf

[10] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, 684.

[11] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347

[12] Bormann, C., Castellani, A. P., & Shelby, Z. (2012). Coap: An application protocol for billions of tiny internet nodes. IEEE Internet Computing, 16(2), 62.

[13] Rghioui, A., Bouhorma, M., & Benslimane, A. (2013). In 2013 5th International conference on information and communication technology for the Muslim world (ICT4M) (pp. 1–5). IEEE.

[14] Ullah, S., Ali, M., Hussain, A. & Kwak, K. S. (2009). Applications of UWB technology. arXiv preprint arXiv:0911.1681.

[15] Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). In Third international conference on availability, reliability and security, 2008. ARES 08 (pp. 642–647). IEEE.

[16] Curran, K., Millar, A., & Garvey, C. Mc. (2012). Near field communication. International Journal of Electrical and Computer Engineering, 2(3), 371.

[17] M. Chen, J. F. Wan, and F. Li, "Machine-to-machine communications: architectures, standards, and applications," KSII Transactions on Internet and Information Systems, to appear, January 2012.

[18] G.Yang, J. Xu,W.Chen, Z. H. Qi, and H.Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.

[19] C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.