International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

The Study on Security in Internet of Things (IoT)

Rishu Jain[1], Ayan Rajput[2], Navneet Singh Chauhan[3]

[1]Scholar, M.Tech (CSE), J.P. Institute of Engineering & Technology, Meerut

[2]Assistant Professor, Computer Science & Engineering Department, J.P. Institute of Engineering & Technology, Meerut

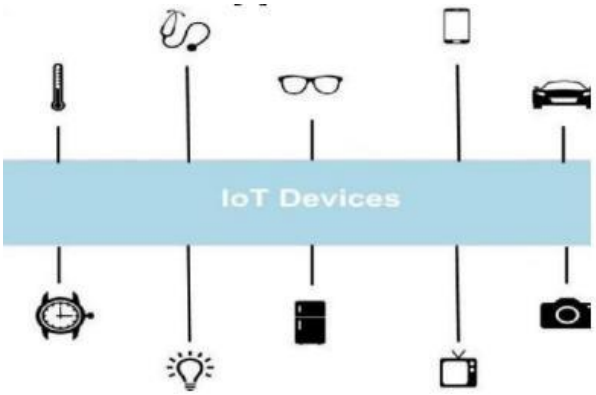
[3]Assistant Professor, Computer Application Department, Shri Ram College, Muzaffarnagar

Abstract: *The Internet of Things, or IoT, has received a lot of attention lately since it has drastically altered human existence. In a wide range of applications, including smart buildings, smart health, smart transportation, and more, the Internet of Things facilitates the sharing of information or data. Sensitive information that may be disclosed is interchangeable among billions of interconnected objects. Thus, maintaining user privacy and bolstering IoT security present a significant issue. This paper aims to provide an in-depth analysis of IoT security. A taxonomy of security requirements depending on the objectives of the attacks is proposed after a number of IoT security threats are studied. In addition, current security solutions are categorised and characterised according to their use cases. In the end, open research directions and security issues are talked about.*

Keyword: Internet of Things (IOT), Wireless Sensor, Security, Privacy, Issues Networks.

I. INTRODUCTION

Kevin Ashton first proposed the idea of the Internet of Things in 1999. The goal of IoT is to connect anything, anywhere, at any time [1]. IoT items range in size from tiny to massive equipment that, in an ideal world, connect with one another online without the need for human involvement [2]. Sensors for data collection and actuators for autonomous, intelligent action execution are features of Internet of Things devices[3]. The Internet of Things (IoT) has drawn a lot of interest in recent years because it has the potential to benefit humans greatly. The major goal of the Internet of Things is to combine these many different application fields into one cohesive whole known as the "smart life" [4]. It is anticipated that billions of gadgets will soon be connected to the Internet [5]. As a result, the volume of data flowing across the Internet will only increase [6]. This data is susceptible to eavesdropping and alteration, among other security threats. The user's privacy will thus be in jeopardy [7].



.

A vast array of physically autonomous sensors that are placed across the environment to monitor and regulate environmental conditions make up a wireless sensor network (WSN) [1]. The WSNs are vulnerable to a variety of assaults, including node tampering, jamming, sinkhole and wormhole attacks, etc. [6].IoT objects are identified and tracked via radio frequency identification, or RFID. It enables short-range radio signal data transfer [1]. RFID technology has numerous vulnerabilities, such as those related to spoofing, cloning, and sniffing, much to WSNs [6]. Because cloud computing provides infinite processing and storage capacity, it plays a significant role in the Internet of Things [10]. An application layer protocol for devices with limited resources is called Constrained Application Protocol (CoAP) [11,12]. Transmission of IPv6 packets across IEEE 802.15.4 networks is made possible by the IPv6 Low power Wireless Personal Area Network (6LoWPAN), which combines IPv6 and LoWPAN [11]. With its many benefits, the 6LoWPAN is worthy of the Internet of Things. But it is vulnerable to several kinds of assaults, such as eavesdropping and DoS (Denial of Service) attacks [13]. Because of its increased precision, security, and low power consumption, Ultra Wide Band (UWB) is a viable technology for a wide range of Internet of Things applications [14].

A protocol for Wireless Personal Area Networks (WPANs)' physical layer and MAC (Medium Access Control) layer is IEEE 802.15.4. It offers the connection between low-energy-consuming items in the home [11]. Short-range technology called near field communication (NFC) is utilised in many Internet of Things applications, including payment and authentication systems. Data interchange and network access are made simple by the NFC. However, because an attacker might intercept the wireless signal the device creates, it is vulnerable to information leakage [15,16].

At this point, autonomous control and ambient intelligence are not part of the original Internet of things notion. There is a movement in M2M research that integrates the concepts of IoT and autonomous control to develop an advancement of M2M in the form of CPS. This shift is due to the expansion of improved network techniques and cloud computing. To satisfy the increased standards for security, dependability, and privacy, new techniques and technologies need be created [3].

II. Security

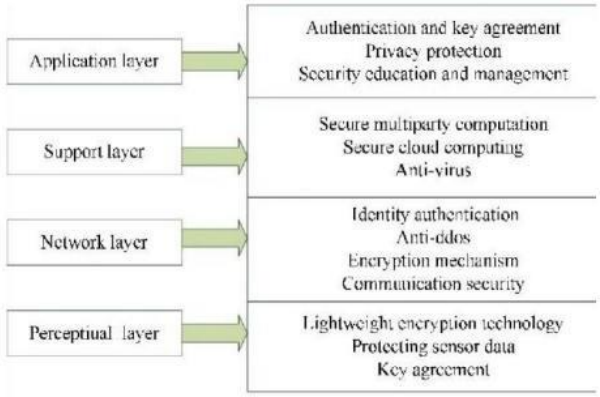
A wireless sensor network (WSN) is made up of a wide range of physically independent sensors that are positioned across the environment to track and control environmental conditions [1]. The WSNs are susceptible to many attacks, including as jamming, sinkhole and wormhole attacks, node tampering, etc. [6].Radio frequency identification, or RFID, is used to identify and track Internet of Things objects. It makes data transfer via short-range radio signals possible [1]. RFID technology is vulnerable to several attacks, including those that target WSNs and involve spoofing, cloning, and sniffing [6]. Cloud computing is important to the Internet of Things because it offers limitless processing and storage capacity [10]. Constrained Application Protocol (CoAP) is an application layer protocol designed for devices with constrained resources [11,12].

The IPv6 Low power Wireless Personal Area Network (6LoWPAN), which combines IPv6 and LoWPAN, enables IPv6 packet transmission across IEEE 802.15.4 networks [11]. The 6LoWPAN is deserving of the Internet of Things because of its many advantages. However, it is susceptible to various types of attacks, including DoS (Denial of Service) attacks and eavesdropping [13]. Ultra Wide Band (UWB) is a promising technology for a variety of Internet of Things applications due to its low power consumption, enhanced precision, and security [14]. IEEE 802.15.4 is a standard that provides a connection between low-energy-consuming devices in the house and the physical layer and MAC (Medium Access Control) layer of Wireless Personal Area Networks (WPANs) [11]. Near field communication (NFC) is a short-range technology that is used in many Internet of Things applications, such as authentication and payment systems. The NFC simplifies network access and data interchange. However, the gadget is susceptible to information leakage since an attacker could intercept the wireless signal it generates [15,16].

Currently, the basic concept of the Internet of things does not include ambient intelligence or autonomous control. A trend in M2M research is developing CPS, a development in M2M that combines the ideas of IoT with autonomous control. This change is brought about by the growth of more advanced network technologies and cloud computing. It will be necessary to develop new methods and technologies in order to meet the raised requirements for security, dependability, and privacy [3].

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 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.

- **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)

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.

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/en/ 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. 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.