INTERNET OF THINGS (IOT) SECURITY ISSUES-A COMPREHENSIVE REVIEW.

Mrs. Asmita H. Hendre. Navsahyadri Group of Institutions, FOM - MCA Bhor, Pune

Dr. Ashwini Brahme. Yashaswi Educations Society's International Institute of Mgmt. Science, Chinchwad, Pune

Mr. Ravikant D. Kale. Navsahyadri Group of Institutions, FOM – MCA. Bhor, Pune

Abstract: As a paradigm-shifting technology, the Internet of Things (IoT) links a wide range of devices to enable smooth communication and data sharing. Significant security issues have emerged along with extraordinary ease and efficiency brought about by the proliferation of IoT devices. Due of its profound impact on human life, the Internet of Things (IoT) has garnered a lot of attention lately. A plethora of applications, such as smart homes, healthcare, transportation, and many more, are made possible by the Internet of Things. The concept of "smart life" can be formed by combining these several application sectors. Cybercriminals and security professionals are in a race as a result of the IoT quick development. Due of the communication and exchange of potentially sensitive information across billions of linked devices. Consequently, enhancing IoT security and protecting user privacy present significant challenges. In-depth research on IoT security is the goal of this study. After examining many IoT security assaults, a classification of the security conditions built on the goals of the incidents is suggested. Corresponding to the function areas in which they are employed, recent security solutions are also described and organized into categories.

Keywords: IoT, Security, Privacy, Smart life, Cyber-attacks.

Introduction**:**The Internet of Things was first proposed by Kevin Ashton in 1999. Thanks to the Internet of Things, anything can be connected at any time or place (Gubbi et al., 2013). The Internet of Things, or IoT, is a term used to describe physical items that can be very little or very large in size and can connect with each other through the Internet without the need for human contact (Yan et al., 2014). Actuators on Internet of Things devices perform activities autonomously and intelligently, while sensors gather data (Saif et al., 2015). A number of IoT device examples are shown in Figure 1.

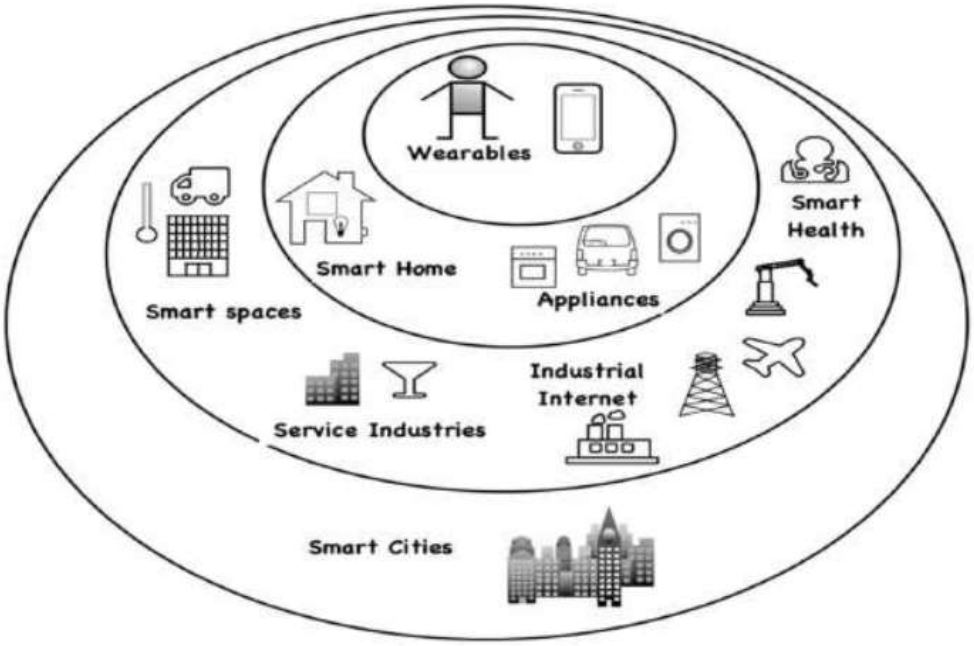

Figure 1: The application of IoT [Source: Google, Gouri Shukla1, Krishna Nand Mishra (2023)]

IoT advances have recently been made possible by the growth of wireless sensor networks, which have a wide range of applications. The development and implementation of the IoT can greatly benefit a wide range of human pursuits, including public health, healthcare, smart grid,

environmental surveillance, and ITS (Intelligent Transportation System). The Internet of Things (IoT) is a huge network of devices with wireless or wired connections that have sensors, or actuators as you might call them. An Internet of things link is a physical connection between two different items (Dargad and Sutar, 2019). One of the main points is that we use new IoT-based technologies in our daily lives and hear about them all the time. Zhou (2010) claims that the term "IoT" refers to a variety of information sensing instruments and technologies, such as gas inductors, RFID, GPS, infrared sensors, laser scanners, and sensors. It collects all processes and objects that must be monitored, linked, and interacted with in real time. It collects information on the various demand variables, including biology, chemistry, geography, mechanics, sound, light, heat, and electricity.

The Internet of Things (IoT) combines a number of existing in use technologies, including as RFID, wireless sensor networks (WSNs), cloud computing, and limited application protocols. It consequently inherits the security flaws of every technology (Andrea et al., 2015). A few of the current technologies are shown in Fig. 2.

- According to Gubbi et al. (2013), a WSN is an array of multiple independently deployed sensors that are physically positioned and utilised for environmental monitoring and control. According to Borgohain et al. (2015), the WSNs are susceptible to a range of attacks, including as jamming, node tampering, sinkhole and wormhole attacks, etc.
- IoT devices are recognised and tracked via RFID. It uses radio waves to facilitate data transfer across short distances (Gubbi et al., 2013). RFID technology is vulnerable to sniffer, cloning, and spoofing attacks, just like the WSN (Borgohain et al., 2015).
- Because cloud computing provides infinite processing and storage capacity, it is crucial to the Internet of Things. (Et al., Botta 2016).
- Al-Fuqaha et al. (2015) state that it offers low-energy connection for personal area products.

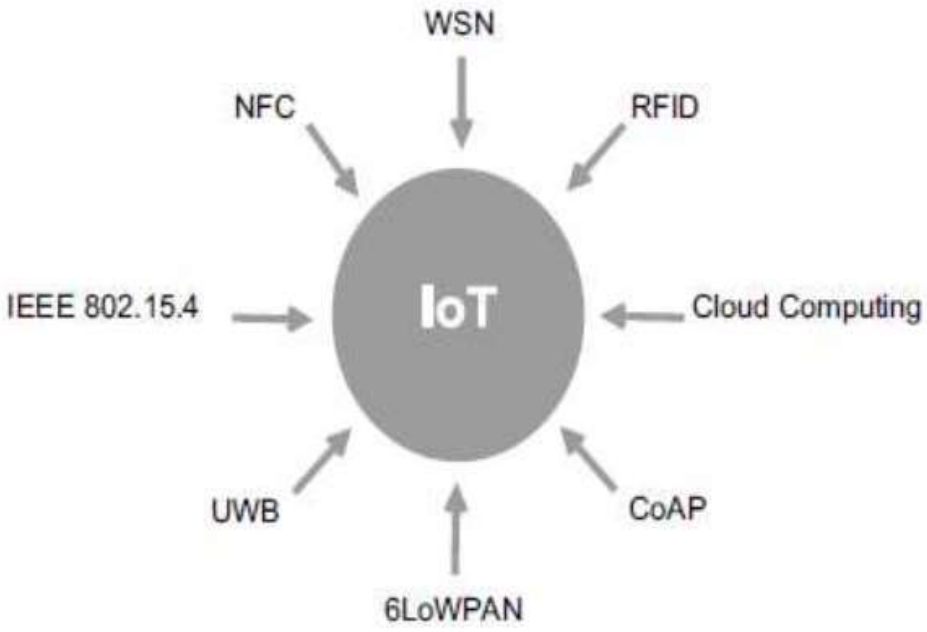

Figure 2: IoT enabling technologies [Source: Google, Sanjeev Kumar Trivedi, Neeraj Kumar Tiwari (2023)]

IoT security is a challenging endeavour. But most IoT devices are designed to be small and have limited resources (battery, processing power, and storage). It is not possible to execute conventional security measures due to their great complexity and difficulty (Cole & Ranasinghe, 2008; Eisenbarth et al., 2007). Developing a lightweight security system for devices with limited resources is the primary challenge.

Methodology: The study is based on an extensive approach that makes use of secondary data analysis. Without the requirement for primary data collecting, this involves looking through

already published research papers, industry reports, and consumer data to obtain insightful information. Selecting accurate and pertinent data is essential to the veracity of the conclusions.

Objectives of the study

- To evaluate and classify the different security risks affecting IoT ecosystems.
- To give a thorough rundown of all possible dangers, such as denial-of-service attacks, device tampering, data breaches, and illegal access.
- To research and talk about cutting edge technologies including encryption protocols, machine learning, and block chains.
- To make suggestions for tightening rules and guidelines in order to guarantee a more secure Internet of Things ecosystem.

Literature Review**:** IoT security was described by Sfar et al. (2018) in a roadmap that took identity, access management, privacy, and trust into account. They started by providing the IoT with a deliberate cognitive technique (Riahi et al., 2014). The authors thought that their plan was more workable and flexible than the tiered approach. They explained the elements and connections of the methodology as well as how effectively it works in smart manufacturing. Following that, they went over a taxonomy of existing security flaws, offered helpful solutions, and suggested numerous lines of inquiry. Lastly, they presented crucial IoT security standardisation procedures. While the study was interesting, it only looked at potential security flaws in the way their approaches interacted; it skipped over other issues related to IoT security, such as availability, integrity, and confidentiality.

Mendez et al. (2017) discussed the current IoT standards' security goals. They established some security guidelines for data and IoT devices. The technologies and protocols that are supported by IoT levels for the application, network, and perception were then covered. When flaws in the technology, like those in RFID and WSN, were found, many fixes were released. In terms of security, they gave priority to data availability, privacy, and secrecy. They also discussed potential solutions and security issues. They did not, however, elaborate on the precise flaws in the enabling technologies. Yang et al. (2017) published a study on the challenges with security and privacy for Internet of Things systems and applications. Their work is divided into four sections. They started by examining the two primary IoT device limits: computational and battery. Secondly, they offered a taxonomy of IoT attacks according to (Andrea et al., 2015; Ronen & Shamir, 2016). Thirdly, the authors focused on access control and verification techniques as well as IoT system architectures. Then, the network layer, transport layer, perception layer, and application layer security vulnerabilities were investigated. This article's writers discussed privacy and security concerns related to IoT. They could only do authentication and access control, though. As a result, a number of crucial security concerns—such as integrity, confidentiality, and privacy—were ignored. Furthermore, they provided insufficient details on the IoT assaults. Chahid et al. (2017) not only described the application, network, and perception levels, but they also named a few IoT security threats. The writers then offered a few choices that were released by different companies and groups. Finally, they talked about possible next steps before calling it quits. The writers looked into IoT security procedures that are in use now. Nevertheless, they did not give any literature-based solutions; instead, they merely gave a brief description of the security concerns. Moreover, a comprehensive explanation of the security precautions was left out.

They also didn't go into great detail about the possible security risks. Smart homes, healthcare, and industry were some of the IoT applications that Razzaq et al. (2017) covered. The key requirements for Internet of Things security were then enumerated, including privacy, secrecy, access control, and authentication. They then focused on security issues, particularly those that surfaced, classifying these attacks into four groups according to their results and offering some workable solutions for a smart home. Furthermore, the majority of the attacks that were found had no descriptions.

According to the authors of Meng, Y. et al. (2018), the integrity of user data has been jeopardised by a number of issues, including spoofing and jammer attacks as well as other forms of unauthorised access. Potential solutions exist that can assist the user in putting

different security measures in place to help safeguard their Internet of Things devices. Siby, S. claims that a number of privacy risks have surfaced recently and can infiltrate an integrated network using IoT technologies and et al. (2017). Managing the security of IoT devices in companies and organisations is a difficult task. It is imperative for organisations to implement monitoring and scanning technologies for all IoT devices in order to identify potential privacy issues and reduce the likelihood of a breach. Cyber threat detection and analysis are aided by traffic interceptors and analysers.

Numerous research studies and services have been carried out regarding the current developments in IoT security. W.H. Hassan (2019), Various IoT devices and its guards have faced issues or attack vectors due to several services. The development of the unique IoT security protocol can also benefit from the presence of many platforms that can validate this security protocol, modellers, and a variety of simulation tools. It is reasonable to state that research on IoT security has advanced quickly, and this study has been aided by a variety of modelling tools and simulation tools. There will be serious problems if the IoT gadgets malfunctioned.

Despite the vast advantages that users are reaping from the Internet of Things, the authors of Leloglu, E. (2016) contend that there are certain drawbacks that should be considered. The two main issues raised are those related to cybersecurity and privacy. One of the most crucial things to think about, according to Liu, X et al. (2017), is contract termination for devices that use multiple communication protocols. The implementation of individual service contracts is hampered by the disparities in protocols, which are essential components of any Internet of Things cybersecurity framework. Ali, S.; Bosche, A.; Ford, F. (2018)'s writers discussed a few of the IoT cybersecurity solutions that are available now. The supplier states that it is not profitable for the supplier to produce high-quality solutions and implements some rudimentary security measures. Businesses are unlikely to provide the best solution when it comes to Internet of Things cybersecurity.

Security Risks with IoT: Both IoT devices and security breaches are evolving at a rapid pace. To effectively integrate security requirements into IoT systems, a smart place to start is by analysing IoT vulnerabilities and threats. IoT devices are susceptible to various attacks. Furthermore, researchers note that controlling the discourse and gaining access to sensitive or private information are the main goals of many attacks.

Security Challenges: Security companies should be used in Internet of Things applications and systems to guarantee data integrity while packets are routed through several devices and connections to the intended receiver via the internet. Furthermore, since high-power devices make up the majority of IoT devices, the previously suggested cryptographic technique cannot be used in an IoT setting. Security is the most important aspect of any system or application during the planning phase, but nowadays, the integration of any application into network infrastructures is only focused on achieving functionality. Additionally, this opens a backdoor for attackers and opponents. Therefore, it opens the door for such systems and applications to be compromised. As mentioned earlier, experts in cyber security have cautioned that Internet of Things (IoT) is among the most susceptible technologies and that, in contrast to current and emerging infrastructures, there will likely be a great deal more targeted attacks. As an example, there are ransomware assaults for smart watches, cars, homes, and hotels, as well as data theft, system damage, and physical harm. There are four main security issues with every IoT system or application;

(1) Trillion points of vulnerability: Any device connected to the Internet of Things carries some level of risk, and when those risks manifest, it begs the question of how much an organisation can trust the integrity and collection of data. Regarding such risk, this is a topic that is often on everyone's mind.

(2) Trust and Data integrity: This is done in order to ensure that the data hasn't been tampered with in transit from the senders' computers to the intended receiver, or, to put it another way, until it arrives at its intended location. It also takes part in the data verification process to verify the integrity of the data and to validate its verification certificate.

(3) Data protection: For the purpose of protecting data or regulating personal and organisational information collected by applications or sensors and stored in file systems, laws must be developed.
(4) Data privacy: Data privacy is the safeguarding of data from exposure in the setting of Internet of Things devices or applications. For example, each physical or logical object might have a fully own network address allocated to it. The ability to communicate via a network would likewise be extended to such objects or entities.
Finding: In this study, the authors obtain a list of security vulnerabilities, particularly related to IoT. Conducting a Systematic Literature Review is how it's done. IoT is now a need in the modern world. Customers want services delivered right to their door or in a way that requires the least amount of work, consumes less resources, saves them time, is affordable, and is dependable. The key goal is to have everything mentioned above more secure in every way. Thus, IoT can be used to accomplish this. And this can be effectively accomplished by implementing security mechanisms in an efficient manner. As in this assessment, the author identifies the different areas in which further effort is required to establish the credibility of IoT services for the benefit of humankind. An introduction of the key IoT principles is provided in this study, with a focus on the challenges and security issues related to IoT devices. It has been determined that there are vulnerabilities and threats that could keep people from embracing IoT technology.
Conclusion: The proliferation of IoT devices is accompanied by an increase in data volume. The IoT has to overcome a number of security issues that are preventing it from becoming a secure infrastructure. Intelligent object design should also move towards more autonomy in recognising threats and taking appropriate action. Adaptive belief patterns are required in a dynamic, diverse, and all-encompassing ecosystem to enable devices to recognise reliable nodes. Consideration should be given to effective important management in these networks.
Researchers examined IoT security flaws and attacks. Following that, researchers created a taxonomy of IoT security requirements based on the objectives of the attackers. Researchers and developers can use this nomenclature to help them come up with new IoT security methods. Review some of the most recent security solutions proposed for particular categories of IoT applications. Lastly, researchers argue that the proliferation of IoT raises a number of security concerns. Developing effective and adaptable security measures for machines with limited resources is the main problem.
Future Work: Subsequent studies ought to evaluate the security implications linked to the Internet of Things and investigate if users will take precautions to protect themselves when utilising it. Everyone must also decide whether to respect and employ administrative tools that specifically stop IoT device security invasions. It's difficult to make IoT systems more safe, effective, and efficient, especially when managing large amounts of data in real time. As a result, researchers ought to concentrate on improving the IoT-based domain's privacy, security, integrity, efficiency, and dependability.

References

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), 2347-2376.
Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; Bain and Company: Boston, MA, USA, 2018
Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE
Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. arXiv preprint arXiv:1501.02211.
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, 684-700.

Chahid, Y., Benabdellah, M., & Azizi, A. (2017, November). Internet of things protocols comparison, architecture, vulnerabilities and security: State of the art. In Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems (pp. 1-6).
Cole, P. H., & Ranasinghe, D. C. (2008). Networked RFID systems and lightweight cryptography. London, UK: Springer. doi, 10, 978-3.
Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., & Uhsadel, L. (2007). A survey of lightweight-cryptography implementations. IEEE Design & Test of Computers, 24(6), 522-533
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), 1645-1660.
Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.
Leloglu, E. A review of security concerns in Internet of Things. J. Comput. Commun. 2016, 5, 121–136.
Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. Future Internet 2017, 9, 27.
Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879.
Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. (2018) Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. IEEE Wirel. Commun. 2018, 25, 53–59.
Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. International Journal of Advanced Computer Science and Applications, 8(6), 383.
Riahi, A., Natalizio, E., Challal, Y., Mitton, N., & Iera, A. (2014, February). A systemic and cognitive approach for IoT security. In 2014 International conference on computing, networking and communications (ICNC) (pp. 183-188). IEEE.
Ronen, E., & Shamir, A. (2016, March). Extended functionality attacks on IoT devices: The case of smart lights. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 3-12). IEEE.
Saif, I., Peasley, S., & Perinkolam, A. (2015). Safeguarding the Internet of Things: being secure, vigilant, and resilient in the connected age. Deloitte Rev 17.
Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.
Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighbourhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30.
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.
Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health internet of things. Journal of Network and Computer Applications, 89, 26-37.
Zhao, K., & Ge, L. (2013). In 2013 9th International conference on computational intelligence and security (CIS) (pp. 663–667). IEEE.