Review

Internet of Things (IoT): Issues and Challenges Ahead

Satveer Kaur[1], Gagandeep Kaur[2*]

[1]Maharaja Agrasen University, PCJ School of Management, Baddi, India; dr.satveerk@gmail.com
[2]Ludhiana College of Engineering and Technology, Department of Business Management, Ludhiana, India; gagansidhu65@gmail.com
***Correspondence:** gagansidhu65@gmail.com

Article History
Received: 27 March, 2022
Accepted: 15 June, 2022
Published: 12 July, 2022

Citation
Kaur, S., & Kaur, G. (2022), Internet of things (IoT): Issues and challenges ahead. *Journal of Business Management, 1*(1), 1-4. https://doi.org/10.56388/bm220712

Publisher's Note
Sci-hall press Inc. stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: The Internet of Things (IoT) is a network of embedded technologies that contain physical items and are used to communicate, think, or interact with internal or external states. It is the new technique of communication and interaction of the states. Rather of human-to-human communication, the Internet of Things focuses on machine-to-machine communication. This paper focuses on study of available literature related to IoT along with issues and challenges of the IoT which is concern of the day. It is the technological world but in order to cope up with technology, it is important to highlight the issues and challenges. Besides this, it is more important to overcome them to stay in touch with IoT devices.

Keywords: Internet of things (IoT), Issues, Challenges, Technology

1. Introduction

The concept of networked devices was first introduced in 1970.John Romkey invented a toaster that could be turned on and off through the Internet in 1990.Siemens released the first M2M cellular module in 1995.Kevin Ashton coined the term "Internet of Things" while working at P&G in 1999, and it has since gained widespread use. The term was first referenced in 2004 in prominent media such as the Guardian, Boston Globe, and Scientific American. The International Telecommunications Union (ITU) of the United Nations (UN) produced the first report on this topic in 2005.The Internet of Things (IoT) was founded in 2008.In Garter's (2011) study, market research firm showed interest in IoT [1].The Internet of Things (IoT) is the networking of physical items with electronics built in their architecture, allowing them to communicate and feel interactions with one another and with the outside world. IoT-based technology will deliver advanced levels of services in the next few years, effectively changing how people live their lives [2]. Medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a few of the categories where IoT is well-established [3].Currently, over 7 billion 'Things' (physical objects) are connected to the Internet. This figure is anticipated to reach 20 billion in the not-too-distant future [4]. Thus, IoT is more useful in the business processes. By using sensors, gateways the business processes can be made more useful and technology oriented. By using the information collected at one place, IoT can be useful for making more significant business Processes.

2. Review of Literature

Jing et al. (2014) focuses on security issues as IoT is based on the Internet, Internet security issues will manifest themselves in IoT [5].Because IoT is made up of three layers: perception, transportation, and application, this paper will look at each layer's security issues separately and try to come up with new problems and solutions. This study also examines cross-layer heterogeneous integration challenges and security issues in depth, as well as discussing and attempting to resolve

IoT security issues as a whole. Finally, this study analyzes and contrasts security challenges in IoT and traditional networks, as well as discussing open security issues in IoT.

Yang et al. (2017) says that the Internet of Things (IoT) is ubiquitous in our daily lives [6]. They are employed in our homes, in hospitals, and outside to control and monitor environmental changes, prevent fires, and perform a variety of other useful functions. However, all of these advantages may come at the expense of significant privacy and security risks. Many research studies have been undertaken to counteract these issues and develop a better solution to eliminate or at least limit the dangers to the user's privacy and security requirements in IoT devices. The survey is divided into four sections. The foremost section will throw light on the important limitations and ways to overcome them. The taxonomy of IoT attacks will be presented in the second. The procedures and architectures for authentication and access control will be discussed in the following segment. The final chapter will look at security challenges at various layers.

Raja et al.(2018) says that The Internet of Things (IoT) is described as a physical or virtual thing or device that is connected and communicates with one another and is incorporated into a network for a specific purpose [7]. Sensors, radio-frequency identification (RFID), and actuators are used in the Internet of Things to collect data. IoT is about more than just gathering data from sensors; it's also about interpreting it. IoT must try to keep attackers from hacking the devices. IoT is about a connected ecosystem where people and things interact to improve the quality of life. It must allow for information sharing while maintaining strict secrecy. IoT infrastructure must be open source and non-proprietary, allowing anybody to build, deploy, and use it. This paper's goal is to explain the numerous challenges, issues, and applications that the Internet of Things faces. Ahmed et al. (2019) examined that the Internet of Things (IoT) is a framework in which each physical thing may be uniquely recognized and can send and receive data via a network [8]. This paper provides an overview and assessment of IoT security, as well as a discussion of its current state and issues. In most IoT architectures, there are three layers: perception layer, network layer, and application layer. A number of security rules should be implemented at each tier for a secure internet of things implementation. The implementation of IoT in the future will only be viable if the security challenges associated with each layer are handled and addressed. A lot of researchers are attempting to address and provide solutions for each tier of IoT security. This paper gives an overview of possible security countermeasures and problems.

Stoyanova et al. (2020) identified the most important issues that arise during the complicated process of IoT-based investigations, including all legal, privacy, and cloud security concerns [9]. This study also provides an overview of past and present theoretical theories in the field of digital forensics. Frameworks that aim to extract data in a privacy-preserving manner or secure evidence integrity using decentralized block chain-based methods are given special attention. The study also discusses the current Forensics-as-a-Service (FaaS) model, as well as several interesting cross-cutting data reduction and forensics intelligence methodologies. Finally, a number of other research trends and unresolved challenges are discussed, with a focus on the need for proactive forensics readiness techniques and widely accepted standards.

Pajouh et al. (2021) examined IoT security concerns, limitations, requirements, and present and future solutions in depth. The study focused on the important IoT issues and challenges [10]. The layered architecture is then used to categorize IoT security concerns and solutions, allowing readers to better understand how to address and implement best practices to avoid the current IoT security dangers on each layer. Malhotra et al. (2021) presents a brief overview of the technology, with a focus on various attacks and anomalies, as well as their detection using an intelligent intrusion detection system (IDS) [11]. The study focused on the technologies based on machine learning. The study was conducted on the health care system. The research examines the architectural, security, and privacy concerns, as well as the use of learning paradigms in this industry. Finally, the research evaluation is completed by listing the results derived from the literature. Furthermore, the study presents a number of research problems in order to enable for additional improvements in approaches to dealing with uncommon complications.

3. Objectives and Research Methodology

The study was conducted in order to fulfill the following objectives:

- To study the various issues in IoT devices, and
- To discuss the challenges in IoT devices.

The study was descriptive in nature. The study was conducted with the help of the secondary data which was collected from books, magazines, journals, research papers and websites related to the IoT.

4. Issues in IoT

Due to the large or small attacks, the security concern of IoT devices has remained a concern for all using IoT devices from the long time. The majority of these assaults are the result of minor security issues, such as the retention of default passwords on a telnet service.

The services of the IoT devices should be available only for trusted people. Most IoT devices fail to provide this type of security. IoT devices seem to be authenticated enough. All connected devices can be trusted. This is especially problematic when the device is connected to the Internet: everyone in the world now has the opportunity to use the device's functionality [12]. The attackers can attack easily on the devices which are providing a number of the services. Availability of more services leads to the more possibility of attacks on the devices. There may be open ports on a device with services running that aren't necessarily necessary for functioning.An assault on such a pointless service might be easily avoided by not exposing it [13]. In case of fixed software vulnerabilities, it becomes difficult to update the version in order to safeguard against the vulnerability.

This means that IoT devices must be sent with up-to-date software that is free of known vulnerabilities, as well as update functionality to patch any vulnerabilities discovered after the device is deployed [14].

When a device communicates in plain text, a 'Man-in-the-Middle' can obtain all information exchanged with a client device or backend service (MitM).Anyone with access to the path of the device can obtain sensitive data easily such as login ID or passwords. When an encrypted version is available is a common issue in this category (HTTPS).A Man-in-the-Middle attack in which the attackers can easily access the information and can alter them privately without the knowledge of other parties [15]. Encryption should also be used to secure sensitive data that is stored on a device (at rest).Lack of encryption while storing API tokens or passwords in plain text on a device is a common flaw. Other issues include the use of weak cryptographic algorithms or the inadvertent use of cryptographic algorithms [16].

Recognizing that software contains vulnerabilities is a critical first step in safeguarding IoT devices. Software allows the users to access the features that were not developed by developers. In some situations, the attacker may be able to run their own code on the device, allowing them to collect sensitive data or attack third parties [17].Security vulnerabilities, like other software problems, are impossible to totally avoid when building software. There are, however, ways to avoid well-known vulnerabilities or lessen the likelihood of them occurring. This provides best practices for preventing application vulnerabilities, such as completing input validation on a regular basis. The majority of IoT devices are essentially general-purpose computers capable of running specific software. It permits the attackers to install their own software that is not part of the device's functionality.When security flaws are discovered, the vendor's response has a significant impact on the outcome. The vendor is responsible for gathering information about potential vulnerabilities, developing a mitigation strategy, and updating devices in the field [18].

The customers see the seller's security concerns as a better communication mode to contact the vendor. When a seller fails to provide contact information on how to proceed in the event of a security breach, it is unlikely to assist in the mitigation of the problem. End users will continue to use the gadget in the manner intended if they are unaware of the limits. As a result, the environment may become less secure. Customers should be informed about software updates regularly as well as how to properly dispose of or resale the device so that sensitive data is not passed on. When it comes to privacy protection, the vendor is crucial. A privacy breach could be caused by the vendor or a connected entity, rather than an external attacker. Without explicit authorization, the vendor or service provider of an IoT device could collect information on consumer behavior for reasons such as market research. There have been several reports of IoT gadgets, such as smart televisions, listening in on domestic discussions [19].

When any device is hacked, the consumption of bandwidth is continuously being normal and remains undetectable. There should be a process to detect such hacking. Most devices lack logging or alerting capabilities that would inform the user of any security issues. As a result, consumers are rarely aware that their device is under assault or has been compromised, making it difficult for them to take protective measures [20].Vendors may encourage secure device deployment by making it simple to configure them safely. Users can be persuaded to configure secure settings by paying attention to usability, design, and documentation. The problem of inappropriate access control, for example, includes the use of insecure or default passwords. One solution is to make user engagement with the device so simple, if not obligatory, that establishing a secure password becomes second nature.

5. Challenges in IoT

There is the risk of hacking the devices and moreover there is no device for detecting the hacking. It is one of the most important issues for concern. As a result, there has been an increase in attacks in which hackers have been able to simply manipulate the algorithms that were supposed to protect people [21]. The manufactures are trying their best to sell their gadgets as quickly as possible, without giving much concern to security. This leads to the inadequate testing and upgrading of the software. If the login credentials are weak then there are more chances of hacking of the data. When the firm uses the business credentials on its own devices, there are more chances of exposing the data to the outsiders [22]. It increases with the use of the devices. The attackers can easily stole the information and can use it for malpractices. It leads to malware [23]. The devices are becoming thinner but the battery life of the devices remains constant. If the devices are becoming thinner, battery life of devices should be expanded [24]. The use of the devices leads to the increase in the cost of the product as well as it takes time to come in the market. This is the most concerning issue of the IoT [25]. The new devices should be developed with security preferences which are a requirement of everyone's concern [26]. When it comes to connecting devices, applications, and cloud platforms, connectivity is the most important consideration. IoT devices should be developed in order while keeping in mind the future technological ideas [27]. The IoT developers must think about how to receive, store and acquire the data with privacy [28].

6. Conclusions

Access control and exposed services are without a doubt the most serious security issues. In addition, IoT devices should use best-practice security features like encryption. Vendors can help consumers and security experts use their goods safely by providing documentation and interacting with them. Devices should be physically secured to make it more difficult for attackers. Finally, if a device is hacked, it should refuse the attacker's programmes and warn the user that something is wrong. Concentrating on these issues will undoubtedly improve the security of IoT devices. Thus, it can be concluded that IoT is facing the security, design and employment related challenges which are the most important concerns of today's scenario.

Conflicts of Interest: All authors declare that they have no conflicts of interest.

References

1. Sharma, N., Shamkuwar, M., & Singh, I. (2019). The history, present and future with IoT. In Internet of Things and Big Data Analytics for Smart Generation (pp. 27-51). Springer, Cham.
2. Misra, G., Kumar, V., Agarwal, A., & Agarwal, K. (2016). Internet of things (IoT)–a technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications (an upcoming or future generation computer communication system technology). American Journal of Electrical and Electronic Engineering, 4(1), 23-32.
3. Sharma, V., & Nayanam, K. (2020). Arduino based Smart Water Management. International Journal of Engineering Research & Technology (IJERT), 9, 652-656.
4. Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S., &Arshad, H. (2021). A review on the security of the internet of things: challenges and solutions. Wireless Personal Communications, 119(3), 2603-2637.
5. 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), 2481-2501.
6. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250-1258.
7. Raja, S. P., Raj Kumar, T. D., & Raj, V. P. (2018). Internet of things: Challenges, issues and applications. Journal of Circuits, Systems and Computers, 27(12), 1830007.
8. Ahmad, M., Younis, T., Habib, M. A., Ashraf, R., & Ahmed, S. H. (2019). A review of current security issues in Internet of Things. Recent trends and advances in wireless and IoT-enabled networks, 11-23.
9. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, 22(2), 1191-1221.
10. Haddad Pajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 14, 100129
11. Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. Sensors, 21(5), 1809.
12. Pereira, P. P., Eliasson, J., & Delsing, J. (2014, October). An authentication and access control framework for CoAP-based Internet of Things. In IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society (pp. 5293-5299). IEEE.
13. Rizvi, S., Orr, R. J., Cox, A., Ashokkumar, P., & Rizvi, M. R. (2020). Identifying the attack surface for IoT network. Internet of Things, 9, 100162.
14. Miloslavskaya, N., & Tolstoy, A. (2019). Internet of things: information security challenges and solutions. Cluster Computing, 22(1), 103-119.
15. Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016, September). A survey on secure communication protocols for IoT systems. In 2016 International Workshop on Secure Internet of Things (SIoT) (pp. 47-62). IEEE.
16. Saleem, J., Hammoudeh, M., Raza, U., Adebisi, B., & Ande, R. (2018, June). IoT standardization: Challenges, perspectives and solution. In Proceedings of the 2nd international conference on future networks and distributed systems (pp. 1-9).
17. Ronquillo, J. G., & Zuckerman, D. M. (2017). Software-related recalls of health information technology and other medical devices: Implications for FDA regulation of digital health. The Milbank Quarterly, 95(3), 535-553.
18. Davis, B. D., Mason, J. C., & Anwar, M. (2020). Vulnerability studies and security postures of IoT devices: A smart home case study. IEEE Internet of Things Journal, 7(10), 10102-10110.
19. Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. Computer law & security review, 32(1), 4-15.
20. Abdel-Basset, M., Chang, V., Hawash, H., Chakrabortty, R. K., & Ryan, M. (2020). Deep-IFS: intrusion detection approach for industrial internet of things traffic in fog environment. IEEE Transactions on Industrial Informatics, 17(11), 7704-7715.
21. Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014, November). IoT security: ongoing challenges and research opportunities. In 2014 IEEE 7th international conference on service-oriented computing and applications (pp. 230-234). IEEE.
22. Barcena, M. B., & Wueest, C. (2015). Insecurity in the Internet of Things. Security response, symantec, 20
23. Azmoodeh, A., Dehghantanha, A., Conti, M., & Choo, K. K. R. (2018). Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized Computing, 9(4), 1141-1152.
24. Maddikunta, P. K. R., Srivastava, G., Gadekallu, T. R., Deepa, N., & Boopathy, P. (2020). Predictive model for battery life in IoT networks. IET Intelligent Transport Systems, 14(11), 1388-1395
25. Rong, W., Vanan, G. T., & Phillips, M. (2016, September). The internet of things (IoT) and transformation of the smart factory. In 2016 International Electronics Symposium (IES) (pp. 399-402). IEEE.
26. Duc, A. N., Jabangwe, R., Paul, P., & Abrahamsson, P. (2017, May). Security challenges in IoT development: a software engineering perspective. In Proceedings of the XP2017 scientific workshops (pp. 1-5).
27. Lee, Y. T., Ban, T., Wan, T. L., Cheng, S. M., Isawa, R., Takahashi, T., & Inoue, D. (2020, December). Cross platform IoT-malware family classification based on printable strings. In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 775-784). IEEE
28. Plageras, A. P., Psannis, K. E., Stergiou, C., Wang, H., & Gupta, B. B. (2018). Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. Future Generation Computer Systems, 82, 349-357.