International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 3 Article 5

March 2022

A study on IoT-related security issues, challenges, and solutions.

Md. Mohtab Alam
PhD Scholar, Eklavya University, Damoh, Madhya Pradesh(M.P), ermalam@rediffmail.com

Mohd. Shahnawaz Ansari
Eklavya University, Damoh, Madhya Pradesh (M.P), shahnawaznbd@gmail.com

A study on IoT-related security issues, challenges, and solutions

Md. MohtabAlam, M.S.Ansari
Eklavya University, Damoh, Madhya Pradesh (M.P)
Email id-ermalam@rediffmail.com

Abstract

The Internet of Things is now being developed to be the most cutting-edge and user-centric technology in the works. Raising both an individual's and society's level of life is the goal of this endeavor. When a technology advances, it always acquires certain flaws, which are always open to being attacked and taken advantage of in some manner. In this work, the problems posed by the Internet of Things (IoT) based on the fundamental security principles of confidentiality, integrity, and availability are discussed. It has also been discussed how an overview of the security restrictions, requirements, processes, and solutions implemented for the challenges generated in secured communication inside the IoT ecosystem. In this paper, the vulnerabilities of the underlying Internet of Things network are brought to light, and many security concerns on multiple tiers of the Internet of Things ecosystem have been examined. Based on the findings of our research into the vulnerabilities that are now present, a variety of potential solutions have been proposed in order to solve the ongoing problems that are plaguing the IoT ecosystem. In addition to that, it provides an overview of the various protocols that are used for security in IoT.

Keyword: Internet of Things,security, privacy, confidentiality, integrity, availability.

1. Introduction

Web of Things (IoT) alludes to the following advancement of the web, concurring to the Web Society [14]. It'll empower a organizing framework that interfaces a expansive number of devices, allowing them to gather information and communicate with one another in arrange to create handled shrewd choices. We should point out that devices refer to any item that has been integrated with the suitable equipment and computer program to supply handling and organizing capabilities, which is an critical qualification. Whereas the Web of Things (IoT) offers associations with devices that they can utilize to oversee their resources and create more effective and cost-effective trade models, it moreover gives organisations with the capacity to put through with one another by means of a assortment of channels. This innovation moreover contributes to the advancement of a hyper-connected society, and it has the potential to improve transportation and mobility [2, 3]. A number of issues of security and privacy, however, must be

solved before the technology can be more widely accepted and used in the real world on a widespread basis. Because of the Internet of Things, we need to have a thorough understanding of the difficulties presented by security and privacy concerns associated with it, as well as an understanding of the possible solutions to these problems. If we do not have a thorough understanding of the difficulties presented by security and privacy concerns associated with it, as well as an understanding of the possible solutions to these problems, we will both be jeopardised. By the end of this essay, we will have a better understanding of some of the security and privacy challenges that have developed in the wake of the Internet of Things (IoT), as well as some of the alternative solutions that have been presented to deal with these difficulties.

Web of Things (IoT) could be a tremendous organize made up of connected systems that incorporate gadgets with restricted asset capabilities. In its most essential shape, the IoT could be a colossal arrange made up of interconnected systems that contain gadgets with constrained asset capabilities.Because of the limited resources that IoT devices have available to them, they are unable to take use of the complete security suites that are available on traditional networks. In this position, one must either build a new security architecture for the Internet of Things or rely on current solutions, which creates a problem for the security community. However, it is critical to make efforts to guarantee that lightweight security solutions are utilised to defend the Internet of Things, in order to avoid the devices' resources being exhausted by security-related activities and their performance being compromised.

In terms of security and privacy, there is a challenge linked with the Internet of Things, and that problem is the difficulty in creating safe and secure communication pathways between devices. A large number of separate components are all running at the same time, which is due to the nature of the technology in which they are contained.

Maintaining proper and secure communication and interaction among the components at the network edge is difficult because of the network edge's proximity to the user's computer. Concerns about data privacy and confidentiality have also been highlighted in relation to the Internet of Things, which has sparked a great deal of debate. It is possible, for example, to use this technology to link a large number of networks together in a cost-effective manner. In contrast, a user may not have complete control over individual networks in the great majority of circumstances, exposing data to a broad variety of secrecy and confidentiality concerns. As an additional benefit to users, the Web of Things (IoT) includes a enormous number of connected

gadgets and systems. Due to the expanding complexity of distinguishing, dissecting, and checking basic components in arrange to guarantee compliance with security prerequisites [12], it is getting to be more troublesome to do so. It is additionally troublesome to attain an worthy degree of secure data stream and believe over a shifted assortment of vertical data innovation foundations.

2. Accessibility and Confidentiality

In addition to the technologies outlined over, there are a number of other basic advances that bolster Web of Things systems. Innovation such as radio recurrence distinguishing proof radio frequency identification (RFID), close field communication near-field communication(NFC), and remote sensor systems wireless sensors networks (WSN)are examples of what is included wireless sensors networks (WSN). When used in combination with Internet of Things networks, RFID technology guarantees that IoT items are outfitted with IDs and keen labels, which enable the items to be handled more readily than they otherwise would be. Aside from that, radio frequency identification(RFID) technology enables Internet of Things products to be loaded with smart chips, which allow the things to sense data in their environment, compute, and communicate with one another and with individuals, among other capabilities. The RFID component, on the other hand, is subject to assaults such as refusal of benefit, listening in, skimming, transferring, and side channelling, all of which have the potential to compromise the security and privacy of Internet of Things users [13].

When it comes to Internet of Things networks, wireless sensor networks (WSNs) are frequently utilized to bolster far off detecting applications and data collecting. The utilize of remote sensor systems wireless sensor networks (WSNs) in such applications is favored since they are cost-effective, energy-efficient, require negligible control, and are equipped with intelligence and processing capabilities [14]. Apart from that, this Internet of Things component is subject to wormhole and neighbour discovery attacks as well as ping flood, ICMP flooding, and syn flooding, among other types of attacks. An example of NFC use is communication with smart cards or access control systems, which requires just a short distance (many millimeters) and moo control and information rate prerequisites. Phishing, client following, hand-off, and information fashioning are all reasonable assaults that take use of the NFC component [15].

2.1 Cybersecurity

When it comes to the Internet of Things, cybersecurity concerns are mostly focused on the issues of confidentiality, authentication, and access control. As defined by this concept, data privacy alludes to the got to guarantee that data is kept mystery which as it were approved clients are able to get to it [16]. For ensuring privacy in the Internet of Things, cryptography has emerged as the most important technology to use. However, authentication is the process of verifying that data has not been altered and has been conveyed by the required sender or creator, which is particular from encryption and unscrambling. As it were approved clients may recover or get foundation, communications, and data, whereas access is focused with ensuring that approved users do not encounter any difficulties in receiving the data [17].

2.2 Security

The traditional view of security, according to researchers such as Brumfitt et al., must be abandoned in arrange to bargain with the security issues related with the Web of Things. This conventional see of security, which centers on transport security as well as physical and cryptographic security as well as application security, is not appropriate for the IoT environment. Additionally, the analyst prescribed that a unused security engineering be actualized that joins light-weight scientific capabilities, inter-device coordination, and a network-based client interface, among other things [18].

An approach for protecting Internet of Things networks has been proposed by Chen et al. (340), on the other hand. Based on ideas established in the restorative and natural areas, this methodology points to improve the security of computer systems by consolidating approaches from other areas. Those who oppose this idea, such as Ding et al., have pushed for permitting IoT frameworks to tackle their independent potential in arrange to self-organize and protect themselves against security dangers. Executing secure confirmation mechanisms into Internet of Things networks may also assist to improve the overall security of the network as a whole. For example, in order to safeguard IoT networks, it may be necessary to verify users using certificate-based credentials. It is impossible to stress the necessity of taking appropriate security safeguards into consideration while developing a key-based authentication technique. As a result, there will be less chance of an attacker exploiting a flaw in the design to get around the authentication procedure [19].

2.3 Challenges

Particular privacy and security concerns have evolved as a result of the growing features and technological capabilities of the Internet of Things, as well as the emergence of systems for interfacing with the Internet of Things. In connection with identification, one of the protection and security concerns of the Web of Things is the risk of partner an identifier such as an address with a individual and their related information [20].Another issue to contend with is that of authentication. When dealing with identity theft, the primary challenge is associated with partner the character with a particular setting that damages the individual's protection by uncovering the distinguishing data to substances exterior of the user's individual circle, subsequently expanding the number of conceivable cyber assault vectors for the individual.Another protection and security issue related with the Web of Things is the capacity to track and find individuals. This is a concern for both individuals and organisations. In this case, it is the assurance and recording of the individual's areas over space and time that constitutes a threat to his or her security. In many cases, consumers may think that their data is being misused or that they have no control over the sharing of their area information [21], in spite of the reality that localization and following are as of now accessible by means of various ways such as web activity or versatile phone GPs area. As a result, the Web of Things (IoT) offers a challenge in terms of insuring awareness of monitoring and control over location data, as well as in terms of ensuring control over location data.

In the field of cybersecurity, two crucial factors are profiling and verification. The Web of Things moreover has critical security and security concerns, notably in the areas of profiling, interaction, and presentation, all of which are in violation of individuals' rights to personal information. According to the International Organization for Standardization (ISO), the Internet of Things (IoT) postures a danger within the collecting of information approximately clients in arrange to recognize their interface through association with other sources of information and profiles. In this case, it is doable to utilize profiling strategies in e-commerce for client personalization, as well as inside focusing on and optimization on the premise of consumers' interface and socioeconomics [22]. Profiling,on the other hand, may result in privacy violations if the information is used for objectives such as delivering unwanted adverts, price discrimination, or social engineering, among other things. Furthermore, the gathering and dealing of client profiles within the information commercial center without the assent of the

person being profiled is seen as an infringement of their right to personal privacy. When private information about an individual user is unintentionally broadcast through the public media, the Internet of Things (IoT) may raise privacy and security issues, resulting in the data being released to unwanted audiences, as has happened in the past. Health care, transportation, and retail are just a few examples of Internet of Things applications that rely largely on human interaction to work successfully [23]. As a result of their public character, most of the tactics used to connect with users and provide feedback information constitute an intrusion into their personal privacy if other people are able to see the data. Consequently, the Internet of Things (IoT) must overcome the impediment posed by the simple disclosure of personally identifiable information [24].

The Internet of Things (IoT) also poses privacy and security issues in the context of life transitions and inventory assaults, among other things. It is possible that changes to the control spheres of an IoT device throughout the device's lifetime will result in the leak of the users' private data that was collected during the device's lifetime [25] due to alterations to the control spheres of the device. In their history logs, smart devices record their interactions with a vast number of services and persons, and the information acquired from these interactions is used to make decisions. A consequence of consumer products being meant to be held by the customer eternally is that the deal or sharing of such gadgets may result in the buyer getting get to delicate data around the past proprietor, so breaching the individual's protection. Subsequently, the plausibility of a stock assault puts the security and security of the Web of Things at peril [26]. Progressively solid IoT organizing capabilities are being created in concert with the advancement of end-to-end vision, empowering keen gadgets to be questioned through the web by both authentic and unapproved parties. It is conceivable for non-legitimate substances to inquiry Web of Things gadgets in arrange to pick up unlawful data around the characteristics and presence of the user's individual impacts [27], and the last-mentioned may abuse the gadget to get this data. It is as a result of this that the Web of Things (IoT) has the potential to reveal an extraordinary bargain of data approximately users' lives and products, posturing a danger to their security and individual protection [28].

3. Solutions to Privacy and Security issues

The foremost successful strategy for fortifying the security and security of the Web of Things ought to be based on guaranteeing the accessibility of less user-identifying information exterior of an individual's claim circle of impact. When it comes to finishing this objective of decreasing the accessibility of such information, the Web of Things may concentrate more on local information handling instead of centralized data preparation, and it may also emphasize expanding flat communication between keen gadgets instead of vertical communication [29].The Web of Things to benefits from existing strategies for protection and security conservation, such as information irritation, client-side personalization, encryption, information secrecy and muddling, and information confusion. In any case, comparable techniques have to be altered to require into thought the scattered nature of information in IoT systems in arrange to be compelling. Keen gadgets ought to too be able of confirming inquiries and reacting as it were to demands from substantial organizations [30], which is something that's as of now missing.This may be accomplished in an IoT arrange by employing a PUFs-based security convention, which can be clarified in assist detail within the area that takes after.it is troublesome to check a gigantic number of contraptions related to IoT frameworks in honest to goodness It is conceivable to essentially increase the security of IoT frameworks by utilizing strong confirmation techniques. The nature of the development takes time owing to the colossal number of contraptions included.To bargain with the trouble and secure against security issues such as a man-in-the-middle assault or assailants interferometer with IoT contraptions in arrange to take information [31], Physical Unclonable Capacities (PUFs) may well be utilized to confirm IoT items. When utilized for key era and assertion in a secure environment, PUFs are a low-cost primitive that will be utilized to spare cash.

When utilizing this setup, it is expected that two Web of Things gadgets will be associated to the same server. For each gadget associated to the organize in address, the server is dependable for keeping a list of challenge-response sets that have happened. Other than the PUF-based key assention framework and the secure communication convention [32], another component of the security design may be a computerized signature framework. When associated to a specific IoT arrange, the framework is able of giving security administrations to that organize by utilizing emit keys to defend the data put away interior the arrange. Keeping in intellect that PUFs are

physical primitives which will be utilized to produce unclonable gadget particular estimations on Coordinates Circuits is basic to understanding the subject matter. To empower the recognizable proof and verification of network devices, the one of a kind estimations may be utilized as fingerprints on the gadgets themselves, permitting them to be perceived [33].

4. Conclusion and Future Scope

When it comes to the Internet of Things networks, security is a major worry that has to be tended to on the off chance that the systems are to be acknowledged and utilized in an assortment of human activity sectors such as commerce and entertainment. With the help of the PUFs-based security protocol, it is possible to identify and authenticate Internet of Things devices. This protocol makes use of interesting keys and timestamps to confirm hubs and messages exchanged interior a particular arrangement.Authentication and identification of Internet of Things devices are two of the most promising technologies that may be utilized to accomplish this. As applied to Internet of Things networks, the approach is constrained in that it requires a considerable sum of computer assets to confirm all of the things, messages, and gadgets within the arrangement, which is restrictively costly. Furthermore, the utilization of a confirmation server may result in the establishment of a bottleneck, which may result in decreased performance.

Reference

1. Khvoynitskaya, S. The History and Future of the Internet of Things. 2020. Available online: https: //www.itransition.com/:https://www.itransition.com/blog/iot-history (accessed on 25 March 2020).
2. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. 2018, 78, 544–546.
3. Monther, A.A.; Tawalbeh, L. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. Int. J. Electr. Comput. Eng. 2020, 10, 2088–8708.
4. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things. IEEE Commun. Surv. Tutor. 2018, 21, 1636–1675.
5. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. IEEE Wirel. Commun. 2018, 25, 53–59.

6. Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. 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.
7. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.
8. Leloglu, E. A review of security concerns in Internet of Things. J. Comput. Commun. 2016, 5, 121–136.
9. 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.
10. 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. Appl. Sci. 2020, 10, 4102 16 of 17
11. Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
12. Izzat, A.; Chuck, E.; Lo'ai, T. The NICE Cyber Security Framework, Cyber Security Management; Springer: Basel, Switzerland, 2020; ISBN 978-3-030-41987-5.
13. Tawalbeh, L.A.; Tawalbeh, H. Lightweight crypto and security. In Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications; Wiley: West Sussex, UK, 2017; pp. 243–261.
14. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. 2017, 88, 10–28.
15. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. 2016, 18, 2027–2051. Available online: https://ieeexplore.ieee.org/abstract/document/7442758 (accessed on 10 April 2020).
16. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.
17. Zaldivar, D.; Tawalbeh, L.; Muheidat, F. Investigating the Security Threats on Networked Medical Devices. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6 January 2020; pp. 0488–0493.
18. Tawalbeh, L.A.; Somani, T.F. More secure Internet of Things using robust encryption algorithms against side-channel attacks. In Proceedings of the 2016 IEEE/ACS 13th

International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.

19. Dalipi, F.; Yayilgan, S.Y. Security and privacy considerations for IoT application on smart grids: Survey and research challenges. In Proceedings of the in Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 63–68.
20. Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016; pp. 172–17.
21. Culbert, D. Personal Data Breaches and Securing IoT Devices. 2020. Available online: https://betanews.com/ 2019/08/13/securing-iot-devices/ (accessed on 15 September 2019). 22. Hu, C., Zhang, J., Wen, Q.: An identity-based personal location system with protected privacy in IoT. In: Proceedings—2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, IC-BNMT 2011, Shenzhen, China, pp. 192–195 (2011).
22. He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the Evolutionary Computation (CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021.
23. Al Shuhaimi, F.; Jose, M.; Singh, A.V. Software-defined network as a solution to overcome security challenges in IoT. In Proceedings of the Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 491–496.
24. Estrada, D.; Tawalbeh, L.; Vinaja, R. How Secure Having IoT Devices in Our Home. J. Inf. Secur. 2020, 11.
25. Alcaide, E., Palomar, J., Montero-Castillo, A.: Ribagorda, anonymous authentication for privacy-preserving iot target driven applications. Comput. Secure. **37**, 111–112 (2013).
26. Tawalbeh, M.; Quwaider, M.; Tawalbeh, L.A. Authorization Model for IoT Healthcare Systems: Case Study. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 337–342.

27. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. 2018, 74, 340–354.
28. Singh, J.; Thomas, F.J.-M.; Pasquier, J.B.; Ko, H.; Eyers, D.M. Twenty security considerations for cloudsupported Internet of Things. IEEE Internet Things J. 2016, 3, 269–284.
29. Cherkaoui, A., Bossuet, L., Seitz, L., Selander, G. Borgaonkar, R.: New paradigms for access control in constrained environments. In: 2014 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), Montpellier, pp. 1–4 (2014).
30. Veltri, L., Cirani, S., Busanelli, S., Ferrari, G.: A novel batch-based group key management protocol applied to the internet of things. Ad Hoc Netw. **11**(8), 2724–2737 (2013).
31. Sicari, S., Rizzardi, A., Cappiello, C., Coen-Porisini, A.: An NFP model for internet of things applications. In: Proceedings of IEEE WiMob, Larnaca, Cyprus, pp. 164–171 (2014).
32. Verma, H., Chahal, K.: A review on security problems and measures of Internet of Things. In: 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, pp. 71–76 (2017).
33. Ivan, T., Dušan, B., Komlen, L., Miodrag, B., Ivana, O.: Security Mechanisms in IoT (2017