Security in Internet of Things (IoT): Challenges and Models

Navdeep Lata [#1], Dr. Raman Kumar [*2]
[#]*Research Scholar, Department of Computer Science and Engineering,*
I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India.
** Assistant Professor, Department of Computer Science and Engineering,*
I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India.
[1]*ernavdeeplata@gmail.com*
[2] er.ramankumar@aol.in

Article Info
Page Number: 75 – 81
Publication Issue:
Vol 71 No. 2 (2022)

Article History
Article Received*: 05 December 2021*
Revised*: 12 January 2022*
Accepted*: 02 February 2022*
Publication*: 11 March 2022*

Abstract
The Internet of Things (IoT) has grabbed the attention of the scientific community in recent years. IoT is a recently formed technology that will be the future of the web, allowing distinct everyday objects to communicate with each other without any human interaction. It is one of the most hotly debated fields in both academia and industry for current and future study areas. IoT security and privacy issues have proven to be critical objectives. This paper includes IoT models, schemes, and implementation issues related to different IoT technologies and devices. It focuses on security challenges of IoT communications such as privacy, authentication, integrity of data, and service availability, mostly in hardware aspects. Attacks and modern vulnerabilities, as well as countermeasures, are taken into account. Various IoT security models are described along with security challenges.

Keywords: IoT Security, Models, Challenges.

1. Introduction

Internet of Things (IoT) is a highly revolutionary innovation with exponential rise, massive influence, and potential. Any deployment of IoT in everyday life demonstrates its future significance. It keeps increasing as technology advances, such as increasing channel capacity by integrating cognitively radio-based connections to handle frequency spectrum underutilization. The IoT connects many network devices to offer emerging applications. IoT devices are diversified, ranging from smart objects to low-power gadgets. IoT gadgets are little installed frameworks that are integrated into products that we use on a daily basis. Sensors and various segments are regularly used in these devices, which may be monitored and controlled via systems and the Internet. IoT devices are commonly utilised to create "smart" frameworks (Damghani et al., 2019). The aim of Internet of Things is to develop a secure and trustworthy "Things" exchange platform. Despite the fact that Internet of Things devices have made living easier, their security has received little attention. The primary goal of developers at the time is to enhance the capacity of devices, with little emphasis on device security. The data sent through the IoT network is at risk of being hacked. Such information is necessary to protect the user's privacy(Khari et al., 2019). Because the consequences of IoT

failures can be catastrophic, studying and researching security concerns in the IoT is essential. As a result, with the help of accessible simulation models, domain experts, and analytical and computational platforms, IoT security research has recently garnered considerable attention. Recently, considerable efforts have gone into handling with security vulnerabilities in Iot network. Some of these approaches focus on a specific layer of securety, while others strive to deliver end-to-end security for IoT(Hassan, 2019). However, some difficulties are becoming more prevalent, and their remedies are unclear. The IoT is posing an increasing number of issues in terms of technological security. Many solutions for securing IoT technologies were created, but there are still several more that could be established. This paper presents security challenges while deploying IoT applications and different categories of security models for IoT.

2. IoT Security Challenges

Heterogeneity in the IoT covers a broad spectrum of hardware resources such as Processor computation power and storage capacity as well as interfaces, frameworks, and rules. The lack of a standard security tools is the most serious concern. We see a future in which IoT devices are virtually integrated in the landscape around, producing massive amounts of data. To form the data meaningful and valuable, it has to be maintained and processed securely. Thus, to implement IoT applications, there is need to study IoT security challenges which are different from conventional networks. These challenges are mentioned below and shown in Figure1.

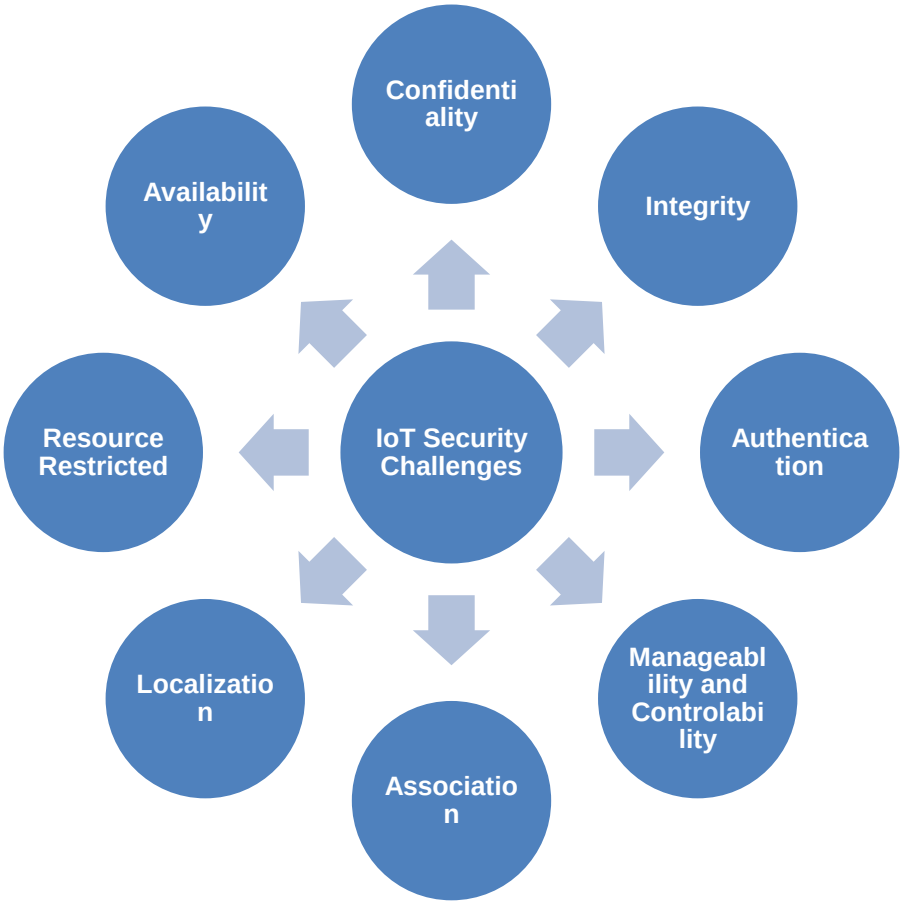

Figure1: IoT Security Challenges

Confidentiality: Because IoT information flows via numerous nodes in a network, it necessitates the use of an encrypted communication mechanism to protect data. The information saved on the IoT device is

exposed to violations of secercy by compromised nodes in IoT network due to a diversified integration of devices, services, and networks. The message is only revealed to authorized ones that may be servers, clients, gadgets, administrations or any other network device; the secrecy is about device and message access control. Unapproved aspects must be kept at a minimum when it comes to private information, keys, and security credentials.

Integrity: Because IoT devices are vulnerable to various threats, an intruder could compromise data integrity by modifying saved data for malevolent objectives. To form the data meaningful and valuable, it has to be maintained and processed securely. Thus, to implement IoT applications, there is need to add sevurity tool which provide integrity.

Authentication: To secure communication in the Internet of Things, authentication is required among two entities. In need to have trusted access to services, the entities must be authorised. Because of the various heterogeneous underlying architectures and ecosystems that support IoT devices, there is a wide range of authentication solutions for IoT. These situations for creating a single worldwide IoT authentication scheme make difficult. Similarly, permission processes ensure that only those who are authorised have access to systems or data. A trusted environment is created by properly implementing permission and authenticity, which assures a highly secured environment. In addition, resource consumption, auditing and logging provide a trustworthy infrastructure for IoT network security(Hassan, 2019).

Availability of Services: Through denial-of-service attacks against IoT devices can restrict the supply of related services. Several tactics, such as sinkhole, jamming attack, and replay assaults, exploit IoT entities at various stages to degrade the quality-of-service (QoS) offered to subscribers(Zhang et al., 2019).

Resource Restricted: IoT devices are often resource restricted, with minimal power and limited memory. By flooding the traffic on network and draining IoT devicess through duplicate or fraudulent calls, threats on IoT systems may lead towards higher energy usage.

Manageability and controllability issues: The major structural difference between an IoT network and a regular network is that the former has manageability and controllability issues. The growth of the Internet of Things has been greatly hampered as a result of this. The Internet of Things must be connected; not only wired but also wireless link connections are used to communicate between the three layers of the Internet of Things. Ethernet, WiFi, Bluetooth, and ZigBee are examples of heterogeneous communication technologies. IoT connects a large number of disparate smart devices. On the one hand, this heterogeneity makes network and IoT application administration extremely difficult. Rapid expansion of heterogeneous networks based on IoT may reveal many of single-points-of-failure, resulting in deterioration of IoT-based services. It necessitates the creation of a contaminate environment for a huge number of Connected devices, as well as alternate ways for fault-tolerant network deployment (Gunathilake et al., 2020; Zhang et al., 2019).

Association: Associating an identity with a specific entitiy may be a threat because it might lead to profiling and tracking. Thus, the most significant issue is to prohibit such conduct in the IoT and implement certain preventative measures.

Localization: Next issue is localization, that occurs when computers try to determine and log a user's whereabouts at some instant i.e., over time and place. Designing techniques for interactions with IoT discourage such action, is among the primary difficulties of security protocols for IoT network. In e-commerce services, profile information of a specific individual to predict interests through association with

other profiles and such data is very frequent. The balancing of company interests in profiling and data analysis with user privacy obligations is a major challenge (Hameed et al., 2019)

3. Security Models

Privacy in IoT is a critical security problem that requires immediate attention from academic and business researchers. Proposals for protocols and management frameworks to handle privacy in IoT are urgently needed. IoT is being used in a variety of applications, including remote healthcare monitoring, energy consumption management, traffic management, and smart parking systems. Users require security of private information relating to their mobility, habits, and connections with other individuals in all of these services. Identity secrecy, geo-location confidentiality, nodes penetration threat, layer removing/adding threat, forward and backward security, and semitrusted and malicious cloud protection are among the security protocols highlighted by the researchers in cloud-based IoT. Thus, there are various types of security models which have different objectives as mentioned below and shown in Table1.

Blockchain-based models

The ELIB approach provided here creates an interconnected network in which highly equipped devices can connect to a public BC that ensures focused privacy and security. The described ELIB model implements a set of three optimizations, including a lightweight consensus method, certificateless (CC) cryptography, and a Distributed Throughput Management (DTM) scheme. In terms of energy consumption, processing time, and overhead, a detailed simulation is run under several circumstances. When compared to the baseline technique, the ELIB saves a total of 50% in processing time with a minimal energy consumption of 0.07mJ(Mohanty et al., 2020). Another model addresses all types of intrusion detection technology in detail, as well as the past and present state of detection techniques. It also defines intrusion detection system categorisation and the structure of general intrusion detection. Intrusion detection technology is a type of security technology that guards network resources against hacker attacks. IDS is a good complement to the firewalls since it may assist the network system catch threats faster and enhance the data security infrastructure's authenticity. Intrusion detection technique is used to a block chain data protection, and the findings reveal that the presented method has improved detection performance and fault - tolerant(Li et al., 2019). A detailed review has been mentioned in (Khan & Salah, 2018; Mohanta et al., 2020).

Cryptography-based models

With the goal of conserving energy of nodes, the research tries to improve MQTT privacy by limiting data manipulation, spying, and impersonation threats utilising Elliptic Curve Cryptography (ECC), system logs, and waking routines. The results will determine that by applying energy and security levels jointly, it is easy to expand the device's lifespan(De Rango et al., 2020). Another new approach is important for the secured transfer of data of disease diagnosis that are interspersed with health records. In elliptic curve cryptography, the ideal key will be determined utilising hybrid swarm optimizer, i.e. grasshopper and particle swarm optimizing, to increase the secure communication of the encrypted communications and decoding process. Healthcare pictures are safeguarded in the Iot infrastructure using this way. The results of this execution are compared and contrasted, and a variety of encryption algorithms with their optimization techniques from the research are found with the most intense max signal-to-noise ratios, 59.45 dB and structural similarity index of 1(Elhoseny et al., 2020).

Deep Learning-based Models

A review of various deep learning based models has been discussed in (Amanullah et al., 2020). The authors undertook a thorough investigation of cutting-edge deep learning, big data technologies and IoT security. Another deep learning-based retrieval technique is to create IoT data processing better using recurrent neural network. Furthermore, in the domains of adversarial learning algorithms, this work proposes a study on querying solutions to prevent hacks by attackers. It also suggests new techniques to using this paradigm in IoT scenarios that are focused on adversarial deep learning(Lin, 2020). Furthermore deep learning techniques for Threat detection and assessed them using the newest CICIDS2017 databases, with the overall performance of 97.16 percent. The developed methodology was also analyzed to machine learning methods. In addition, this report addresses areas for future research for using deep learning algorithms in IoT data security (Ahmed & Askar, 2021; Roopak et al., 2019).

Physical Security-based Models

The goal of this study is to create a standard information security paradigm for collaborative virtualization in the Internet of Things. The study examines network security flaws, challenges, cyberattacks, and liabilities in switches, firewalls, and routers, as well as a policy for mitigating those risks. The essentials of a secured network infrastructure are covered in this paper, including firewalls, routers, AAA servers, and VLAN architecture. In the IoT, it introduces a revolutionary security framework for defending the network against local and global assaults and risks. The developed framework is investigated using a testbed, and the results of the evaluation reveal adequate security and better network efficiency(Alabady et al., 2020). Another system that use smart contracts on the Ethereum blockchain to establish an authentication scheme that aids in the maintenance of dispersed IoT environments through their lifespan. For robust IoT devices, our process guarantees secure maintenance, deployment, communication and management. A smart contract approach for defining and managing basic IoT activities is also proposed. The Ethereum framework is used for permission, communication and authentication in this system, which allows users to manage gadgets. Even without direct human-to-device connection, this architecture enables the devices to work independently by analyzing jobs obtained via smart contract activities. As a consequence, a system with methods for access, job allocation, and audit logs has been developed(Wickström et al., 2021).

Table 1: Security Models for IoT communication

Security Models	**Research**	**Security Challenges**
Blockchain	(Khan & Salah, 2018; Mohanta et al., 2020; Mohanty et al., 2020)	Data security, less energy consumption, reduced processing time, and less overheads
Cryptography	(De Rango et al., 2020; Elhoseny et al., 2020)	Encryption, Optimization, Confidentiality, Secure data transfer
Machine Learning	(Amanullah et al., 2020; Lin, 2020; Roopak et al., 2019)	Querying solutions to prevent hacks, better data processing,
Physical Security	(Alabady et al., 2020; Wickström et al., 2021)	Local and Global threats, Access control, job allocation, and audit logs

Conclusion

IoT is solely based on the sensor-based technologies in which the need to integrate the security that is a core task. In this paper, various security challenges have been identified. In addition, different types of security models have been discussed. The domain of network security related models of cryptography, deep learning, machine learning, blockchain and hash functions are quite enormous and there is need of research as there are so many challenging issues still present. Different models provide different solutions. In future, there is needed to look into worldwide standards for IoT security to ensure connectivity amongst a wide range of security frameworks, gadgets, regulations, and so on. In order to be resilient to thefts and other malevolent threats, IoT Systems require truly innovative network designs.

References

[1]. Ahmed, K. D., & Askar, S. (2021). Deep Learning Models for Cyber Security in IoT Networks: A Review. *International Journal of Science and Business*, *5*(3), 61–70.

[2]. Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A novel security model for cooperative virtual networks in the IoT era. *International Journal of Parallel Programming*, *48*(2), 280–295.

[3]. Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., Akim, N. M., & Imran, M. (2020). Deep learning and big data technologies for IoT security. *Computer Communications*, *151*, 495–517.

[4]. Damghani, H., Hosseinian, H., & Damghani, L. (2019). Cryptography review in IoT. *2019 4th Conference on Technology In Electrical and Computer Engineering (ETECH2019)*.

[5]. De Rango, F., Potrino, G., Tropea, M., & Fazio, P. (2020). Energy-aware dynamic Internet of Things security system based on Elliptic Curve Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. *Pervasive and Mobile Computing*, *61*, 101105.

[6]. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2020). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural Computing and Applications*, *32*(15), 10979–10993.

[7]. Gunathilake, N. A., Al-Dubai, A., & Buchana, W. J. (2020). Recent advances and trends in lightweight cryptography for iot security. *2020 16th International Conference on Network and Service Management (CNSM)*, 1–5.

[8]. Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications*, *2019*.

[9]. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283–294.

[10]. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411.

[11]. Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 73–80.

[12]. Li, D., Cai, Z., Deng, L., Yao, X., & Wang, H. H. (2019). Information security model of block chain based on intrusion sensing in the IoT environment. *Cluster Computing*, *22*(1), 451–468.

[13]. Lin, T. (2020). Deep Learning for IoT. *2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC)*, 1–4.

[14]. Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*, 100227.

[15]. Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems*, *102*, 1027–1037.

[16]. Roopak, M., Tian, G. Y., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0452–0457.

[17]. Wickström, J., Westerlund, M., & Pulkkis, G. (2021). Smart contract based distributed IoT security: A protocol for autonomous device management. *2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*, 776–781.

[18]. Zhang, J., Chen, H., Gong, L., Cao, J., & Gu, Z. (2019). The current research of IoT security. *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, 346–353.