Security of the Internet of Things

Subjects: Computer Science, Cybernetics

Contributor: Hamed Taherdoost

Due to the widespread use of the Internet of Things (IoT), organizations should concentrate their efforts on system security. Any vulnerability could lead to a system failure or cyberattack, which would have a large-scale impact. With billions of interconnected devices, ensuring robust security measures is crucial to safeguard sensitive data, protect user privacy, and mitigate potential cyber threats. Failure to prioritize IoT security could have far-reaching consequences, jeopardizing individuals, organizations, and even critical infrastructure. IoT security is a protection strategy and defense mechanism that protects against the possibility of cyberattacks that specifically target physically linked IoT devices. IoT security teams are currently dealing with growing difficulties, such as inventories, operations, diversity, ownership, data volume, threats, etc.

Internet of Things security data security network security

1. Introduction

The world has experienced some significant technical advancements in computer networking during the twenty-first century, which is known as the age of wireless communication and interconnectivity. Kevin Ashton first used the phrase “Internet of Things (IoT)” in 1999 [1]. IoT is a recent technology that enables the development of networks connecting various items, whether in the real world or the digital one [2]. IoT devices, which range in size from tiny wearables to massive machinery and are outfitted with actuators and sensors, can intelligently sense their environments and take action on their own [3][4].

There will be an increase in the number of IoT applications and gadgets because more sectors are utilizing IoT apps. Wearable technology with devices to monitor and share a person’s behavior and health information is one such business that is providing wearable technology. IoT apps and gadgets are being made available to patients in the healthcare industry [5]. Currently available “smart house” IoT products include smart refrigerators, smart heating, smart gardening, video doorbells, personal assistants for smart lights, smart coffee makers, and smart door locks. Smart parking, smart street lights, and smart trash management are some of the “smart city” apps and IoT gadgets that have been developed [6].

IoT security has garnered a lot of interest in the scholarly community. The security of IoT devices has been a hot topic among academics [7][8][9][10][11][12][13]. IoT has many advantages, but it also has three main problems: data transmission, data gathering, and data security. Many tracking apps have been created specifically to collect data from IoT devices. IoT devices can connect to current networks and exchange data thanks to various protocols that have been developed and changed to transmit gathered data. However, they do not offer these protocols the

attention they require. As a result, IoT is closely linked to many modern and traditional security problems, including identification, data security, permission, etc. Denial of service assaults, replay attacks, Denning-Sacco attacks, password guessing attacks, etc. can all result from login flaws. On the other hand, it is very difficult to authenticate IoT devices across heterogeneous and linked networks. These protocols should also consider problems with IoT device limitations, energy consumption, limited memory space, and limited computing power [14][15][16][17][18][19].

2. Security of Internet of Things

2.1. IoT

A remotely controllable toaster that was first introduced in 1990 was the first basic gadget in this IoT category [20]. A Radio Frequency Identification-based system for item identification was the first widespread smart device application ten years later [21]. The variety of IoT smart applications has fully transformed the network world. Smart finance, smart grids, smart health care, and other smart services are examples of these uses [22]. Numerous applications of the IoT have revolutionized the industry. Predictive maintenance is one of the most important applications of the IoT in industry, where IoT sensors are used to monitor apparatus and machinery and determine when maintenance is required, thereby reducing downtime and increasing efficiency. IoT sensors can also be used to track assets such as products, containers, and vehicles in real-time, allowing for greater supply chain visibility and control. In addition, IoT sensors may be employed to monitor and optimize energy consumption, resulting in cost savings and a smaller carbon footprint. The technology is also suitable for the remote control and monitoring of industrial processes, tracking inventory levels, and automatically ordering supplies when stock is low. In addition to monitoring and detecting potential safety hazards, such as equipment malfunctions or gas leakage, IoT devices can also warn workers of potential dangers.

Numerous and diverse IoT applications in the industry offer significant advantages in the form of cost reductions, productivity, and efficiency. As the technology continues to develop, we can anticipate even more innovative IoT applications in the industry. It is important to note, however, that the implementation of the IoT in the industry comes with its own set of challenges, including the high cost of IoT infrastructure, data security and privacy concerns, and the requirement for specialized expertise and abilities for the development and maintenance of IoT systems. For industries to actualize the full potential of IoT, they need to evaluate the advantages and drawbacks of IoT implementation and work towards overcoming these obstacles.

2.2. Security Requirements in IoT

The security aspect of this technology is significant since recent surveys and trends have documented numerous developments in this area. This evolution of the assaulting mechanism has resulted in the development of numerous zero-day attacks [23]. Adversaries typically attempt to circumvent security frameworks by conducting zero-day attacks, which in turn slow down the network and greatly annoy legitimate users [24].

Information assurance can be defined as the practice of ensuring that information systems will function as expected when needed while remaining secure and protected. Information assurance is defined as “measures that safeguard and preserve information and information systems by guaranteeing their secrecy, verification, integrity, availability, and non-repudiation”, according to the National Institute of Standards and Technology [25]. These steps include “providing for the restoration of information networks by integrating security, detection, and response capabilities”. Because IoT-based systems mix a digital information world with a physical equivalent, communication networks, and data resources, these five pillars of information assurance are relevant as security requirements [26].

IoT security requirements are crucial for ensuring the safe and secure operation of interconnected devices and the data they produce. Strong authentication and access control mechanisms to prevent unauthorized access and defend against cyberattacks are essential IoT security requirements. These mechanisms need to be capable of identifying and authenticating users and devices, controlling access to sensitive data, and providing granular permissions to ensure that only authorized entities can access the system. Moreover, data generated by IoT devices should be encrypted and protected to ensure privacy and confidentiality. Additionally, the data should be protected from tampering to ensure its integrity and authenticity. Network and device security is another vital aspect of IoT security. IoT devices and systems need to be protected from network-based assaults. Physical assaults, such as destruction, larceny, and tampering, should also be prevented by IoT devices’ inbuilt security mechanisms.

2.3. Network Security

The IoT combines the physical and Internet-connected worlds to provide intelligent collaboration between physical entities and their surrounding environments. Typically, IoT devices work in a variety of environments to accomplish a variety of goals. Nonetheless, their business needs to adhere to stringent cybersecurity and physical security standards [27][28]. The participation of interdisciplinary components, networks, computations, and so on contributes to the composite character of IoT settings. This broadens the attack areas of IoT-based systems and makes meeting security restrictions more difficult. To meet the expected IoT security requirements, a solution with all-inclusive factors is required. Nonetheless, IoT devices are typically used in congested and open settings. As a result, attackers/intruders can directly reach IoT devices. IoT devices are usually linked across wireless communication networks, where attackers/intruders can impersonate eavesdropping to extract sensitive information from the communication. Because of their limited resources, IoT devices cannot support complex security solutions [29]. As a result, preserving the privacy or security of IoT-based devices is a multifaceted and difficult job that has sparked considerable interest in both scholarly and industrial areas. Given that the primary goal of an IoT-based system is to provide simple access to anyone, anywhere, and at any time, attack surfaces become more vulnerable to different attacks [30].

IoT devices generate vast quantities of data, which are transmitted over networks, making them susceptible to cyber threats. Consequently, securing the network and data in IoT is essential for the safety and security of the entire system. Network security measures provide the foundation for securing data in transit, whereas data security measures safeguard data in transit and at rest. To ensure the secure and safe operation of IoT devices and

systems, it is necessary to employ a comprehensive security strategy that includes both network and data security measures.

2.4. Security of Data

Information assurance is a broad category of security standards or goals that only pertain to particular digital information systems. Because of this, the section goes into great detail about the goals and/or requirements of IoT security. The reasons why these requirements are challenging to meet about Industry 4.0 applications are also addressed, giving readers helpful insights into why the contentious security requirements are challenging to meet using conventional techniques. The requirements for an IoT-based device's security can be summed up as follows.

The digital world will now document data security as an essential security element, and the introduction of IoT will make data security an indispensable aspect of the creation of safe IoT systems. Several works [31][32][33] deemed data secrecy to be a security requirement for IoT data. Nonetheless, data consistency and data access are considered more beneficial than secrecy, particularly in industrial environments [34][35], because they have a measurable business impact. This is an unsuitable point of view in the context of a networked device world, with businesses quickly shifting their offline platforms to be internet-connected frameworks. According to company-based survey studies [36], it was found and proven that data protection is an important motivator for businesses to migrate to Industry 4.0 [33]. Furthermore, it was stated that businesses were hesitant to adopt data-sharing-based methods (such as cloud sharing, prevention, flaw detection, and so on) due to the lack of proof about the security or safety of these methods during the protection of intellectual property. As a result, this highlighted the need for a consistent strategy to safeguard the rational estate of the presence of data-sharing processes. In the early phases, there is widespread agreement that businesses are hesitant to rely on cloud servers for keeping and exchanging IoT data [37]. Nonetheless, the majority of IoT data violations are noticed within businesses rather than at cloud providers. Then, cloud-based storage was developed to reduce the surface of assaults on both the business and cloud sides. However, data loss mitigation has emerged as an additional requirement, identifying four critical processes required for creating an effective solution. Identification, prevention, recording, and notification are among these variables.

The difficulties in this area are linked with three interfering factors: To begin, due to the resource-constrained nature and mobility of IoT systems, data security methods need to operate in a manner that allows for very limited resource consumption. Second, numerous IoT facilities are supported by data sharing; however, in data-sensitive settings, secrecy is of utmost importance, which frequently presents numerous problems. Third, the need for data security increases dramatically, particularly in the case of sensitive IoT services or apps.

IoT security is a protection tactic and defense mechanism that guards against attacks that particularly target physically connected IoT devices. Network security protects the network and the data it contains from intrusions, assaults, and other threats. This is a wide and inclusive term that covers both software and hardware solutions as well as procedures, guidelines, and configurations for network use, accessibility, and threat avoidance in general. Encryption methods are just one aspect of the topic of data protection. Numerous benefits result from the

combination of IoT and the Industry 4.0 paradigm, including better IoT data exploitation. This covers information sharing and other data-dependent operations that might take place anywhere in the system, even outside the organization's borders. While encryption methods enable preferential data exchange, this part elaborates on other strategies for maintaining the confidentiality of IoT data (**Figure 1**). Significant connections exist between the IoT and network security, cybersecurity, and data security. Protecting IoT devices and networks is vital for preventing cyberattacks. Network security protects the networks that link IoT devices. Cybersecurity requires defending the whole IoT ecosystem from cyber assaults, including devices, networks, and apps.

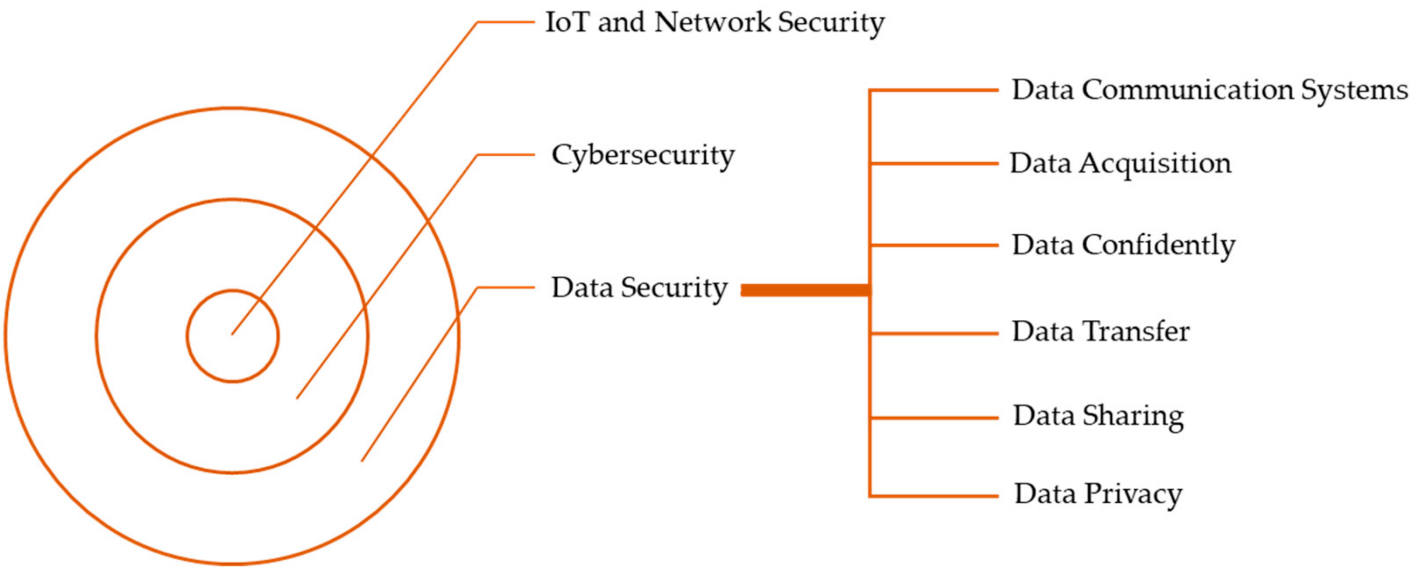

Figure 1. IoT info security: how important is it?

Data security is the safeguarding of data gathered and communicated by the IoT devices. This involves encrypting the data during transmission and storing it securely. In addition, access restrictions and authentication systems are crucial for preventing unwanted access to sensitive data. These data security measures are essential for protecting the data collected and transmitted by IoT devices [38]. IoT devices are susceptible to cyber threats, and protecting them entails installing network security, cybersecurity, and data protection safeguards.

2.5. Summary

IoT software platforms are described as pieces of software that make it easier for IoT devices connected to a network to share data and services. A platform's characteristics [39] include data gathering, integration and storing, tracking, security, event processing, application enablement, processor analysis and visualization, device management, and connectivity and network management. The sanctity of data while in transmission, safe data storage, recognizing devices seeking a link and transmitting data, and permission of users or organizations are the four categories into which security solutions for a network can be broken down. The two types of IoT software platforms are cloud-based platforms and open-source platforms.

A network is created when gadgets are interconnected to carry out specific duties. Both conventional and cellular networks are possible. People can benefit from useful knowledge that is shared or distributed through the network. Utilizing the network is essential for data to be transmitted more quickly. Information security refers to an organization's desire to protect information while it is being transmitted over a network. The confidentiality of data, data veracity, and data exposure to the appropriate individual are the three goals of information security [40].

Data security in the IoT or the cloud is a more recent area of computer security study that can benefit from the established findings in the more established field of data flow management for security [41]. Logrippo [41] approached the issue from a basic standpoint. They demonstrated that, under the assumptions of transitivity and reflexivity, any network of communicating entities can be viewed as a partial order of equivalence classes of entities. This generalized and simplified the current theory, which is based on the lattice concept and generates lattices through labeling. There are many methods to build networks of interacting entities, including routing, access control rules (which may involve naming), etc. For data security, their inherent partial orders were adequate and essential, and in any such network, entities will have varying levels of secrecy or integrity depending on where they are in the partial order. It was demonstrated how labeling systems—which can convey various security requirements—can be built to place things in the proper places within network partial orders. Examples were used to present well-established data security concepts such as disputes, conglomeration, and consolidation. The addition, deletion, or relocation of entities in partial orders as a consequence of occurrences such as user or managerial action was then demonstrated. The preservation of security needs through such transformations was explained using a label-based approach.

Many security-related problems with the current communication technologies need to be resolved to provide safe end-to-end connectivity among services. Additionally, the majority of common security methods that are currently thought to be safe may soon be in danger due to the recent, rapid development of quantum technologies. As a result, for contemporary security systems to withstand various possible quantum computer attacks, quantum technologies need to also be powerful. Quantum walks (QW) are regarded as a global quantum computation model and a top-notch key generator due to their unique properties [42]. In this respect, a novel, lightweight picture encryption method based on QW is suggested in the article by El-Latif et al. [42] for safe data transmission in IoT systems and wireless networking with edge computing. The newly proposed method builds permutation boxes using the power of QW's nonlinear dynamic behavior and creates pseudo-random numbers to encrypt the plain picture after splitting it into blocks. The outcomes of the performed modeling and numerical studies demonstrate the viability of the proposed encryption method. Because of the randomness of the encrypted pictures, it is impossible to decipher them by looking at the connection between neighboring pixels. Additionally, the entropy value is close to 8, the percentage of pixels that change is higher than 99.61 percent, and the key parameters are highly sensitive with a big key area to withstand different assaults. The article by Li et al. [43] developed a data security monitoring method based on narrow-band IoT to address the issues of bad data categorization accuracy and efficacy of conventional data monitoring methods. To begin collecting data for the intranet, a model of network data collection and the best setup for a sensor node were created. Dynamic intranet data analysis indexes were created from three perspectives based on the analysis of data characteristics: creating a security event quantity index, establishing an address entropy index, and data diversion. The security indicator of the IoT was computed

by the narrow-band data aggregation rate previously stated to achieve the security of monitoring data. The testing findings demonstrated that, regardless of whether a network assault is present or not, the technique consistently accomplishes its design objectives in terms of accuracy rate (more than 90%), classification time (less than 4 s), and energy usage (less than 150 J).

IoT frequently offers the data gathering, administration, and device and data protection services needed for application development. IoT things or gadgets interact and compute to improve the comfort and security of our lives. IoT can be used for inventory automation, real-time item monitoring, and the administration of things' information and state. The vast quantity of data that moves between the devices in the network necessitates the creation of a security structure that guarantees the integrity, secrecy, authentication, and permission of data [44]. The sections that follow cover a few data protection solutions.

Authentication

In addition to its inherent limitations such as processing power, storage capacity, and energy resources, the proliferation of IoT devices is raising security vulnerabilities throughout the business. IoT security is becoming a bigger task for security experts to fight attack susceptibility. Given various security flaws, mobile IoT devices require a data routing mechanism to transmit the collected data [45]. The enormous rise in IoT usage has changed daily life in many countries, affecting the entire globe. IoT-based networks require protection just like any other program does because the data they generate contain sensitive data. The security methods currently used in these networks do not consider all security goals. The data need to be protected from different kinds of attacks as soon as they are sensed from the IoT world. Additionally, it needs to be possible to accomplish data integrity, access control, secrecy, and authentication of all concerned parties [46].

Wireless Networks

Wireless sensing networks are a key component of the IoT and have found widespread application in all facets of people's lives. In wireless sensor networks, identity verification ensures users' access to real-time data from sensor nodes without risk [47]. Many tiny devices are used in an IoT-based wireless sensor network (WSN) to gather data and transmit them to central archives. These battery-powered, resource-constrained sensors spend the majority of their energy detecting, gathering, and transmitting data. Security is a major worry in these networks when exchanging data because they are vulnerable to numerous threats, the bloodiest of which is the wormhole assault. These attacks are initiated without obtaining crucial network information, and they seriously jeopardize the network's efficiency, security, and communication. The limited resource availability in the sensing devices makes its prevention more difficult in an IoT-based network context [48]. The ESWI method was created by Shahid et al. [48] to enhance efficiency and security while detecting wormhole attacks. To reduce overhead and energy consumption during operation, this method has been intended to be straightforward and less complex. Their method's simulation findings demonstrated comparable detection rates and packet transport ratios. Additionally, it resulted in significantly reduced energy usage, a decreased end-to-end delay, and improved output.

Use Cases

In network engineering, today's Industrial IoT (IIoT) is very sophisticated, and networks experience annual data leaks. To improve IIoT security defense under privacy regulations, an anti-intrusion monitoring device has been developed. High standards need to be met by the IoT's structural system and security performance parameters are required in an unfriendly network. The network system should employ a technique with a very low rate of data loss and high levels of stability [49]. Teng [49] adopted the first deep-learning network technology after evaluating numerous network designs. The LeNet-5 network was upgraded and optimized by the Convolutional Neural Network technology, and a new LeNet-7 was created. An IIoT anti-intrusion monitoring system was built by combining three network technologies. The system's effectiveness was evaluated and confirmed. The algorithm had a high detection rate, a low false-positive rate, and high data precision. To achieve the highest performance, the model's generality on high-performance data was verified and contrasted with privacy-aware task offloading techniques. As a result, the technology can be used to safeguard IIoT data privacy under the legislation.

Challenges and Prospects

The digital planet can be controlled and monitored thanks to the IoT. The most recent technology to monitor the necessary data is the IoT. IoT is the answer to lowering intricacy and improving system efficiency in transportation, healthcare, and cyber systems. Pervasive computing enables the IoT to handle data and present the necessary graphical user interface. Information can be accessed through a computer system called cloud computing anywhere and anytime on the globe [40].

References

1. Amin, F.; Abbasi, R.; Rehman, A.; Choi, G.S. An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks. Sensors 2019, 19, 2007.
2. Patel, K.K.; Patel, S.M.; Scholar, P. Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. 2016, 6, 6122–6131.
3. Hammoudi, S.; Aliouat, Z.; Harous, S. Challenges and research directions for Internet of Things. Telecommun. Syst. 2018, 67, 367–385.
4. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660.
5. Taherdoost, H. Blockchain-Based Internet of Medical Things. Appl. Sci. 2023, 13, 1287.
6. Chaudhary, S.; Johari, R.; Bhatia, R.; Gupta, K.; Bhatnagar, A. CRAIoT: Concept, review and application (s) of IoT. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–4.

7. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. IEEE Access 2021, 9, 28177–28193.
8. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. Sensors 2020, 20, 3625.
9. Hamad, S.A.; Sheng, Q.Z.; Zhang, W.E.; Nepal, S. Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies. IEEE Commun. Surv. Tutor. 2020, 22, 1372–1391.
10. Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A. A Review of Security in Internet of Things. Wirel. Pers. Commun. 2019, 108, 325–344.
11. Adat, V.; Gupta, B.B. Security in Internet of Things: Issues, challenges, taxonomy, and architecture. Telecommun. Syst. 2018, 67, 423–441.
12. Noor, M.B.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.
13. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.
14. Narayanan, U.; Paul, V.; Joseph, S. Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec. J. Ambient Intell. Humaniz. Comput. 2021, 13, 769–787.
15. Ahmed, M.I.; Kannan, G. Cloud-Based Remote RFID Authentication for Security of Smart Internet of Things Applications. J. Inf. Knowl. Manag. 2021, 20, 2140004.
16. Kumar, P.; Chouhan, L. A privacy and session key based authentication scheme for medical IoT networks. Comput. Commun. 2021, 166, 154–164.
17. Anuradha, M.; Jayasankar, T.; Prakash, N.; Sikkandar, M.Y.; Hemalakshmi, G.; Bharatiraja, C.; Britto, A.S.F. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocess. Microsyst. 2021, 80, 103301.
18. Irshad, A.; Usman, M.; Chaudhry, S.A.; Bashir, A.K.; Jolfaei, A.; Srivastava, G. Fuzzy-in-the-Loop-Driven Low-Cost and Secure Biometric User Access to Server. IEEE Trans. Reliab. 2020, 70, 1014–1025.
19. Chaudhry, S.A.; Farash, M.S.; Kumar, N.; Alsharif, M.H. PFLUA-DIoT: A pairing free lightweight and unlinkable user access control scheme for distributed IoT environments. IEEE Syst. J. 2020, 16, 309–316.
20. Romkey, J. Toast of the IoT: The 1990 Interop Internet Toaster. IEEE Consum. Electron. Mag. 2016, 6, 116–119.

21. Rajaraman, V. Radio frequency identification. Resonance 2017, 22, 549–575.
22. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743.
23. Yu, T.; Sekar, V.; Seshan, S.; Agarwal, Y.; Xu, C. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks, Philadelphia, PA, USA, 16–17 November 2015; pp. 1–7.
24. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187.
25. Nieles, M.; Dempsey, K.; Pillitteri, V.Y. An introduction to information security. NIST Spec. Publ. 2017, 800, 101.
26. Russell, B.; Van Duren, D. Practical Internet of Things Security; Packt Publishing Ltd: Birmingham, UK, 2016.
27. 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.
28. Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics 2022, 11, 2181.
29. Aldweesh, A.; Derhab, A.; Emam, A.Z. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowl.-Based Syst. 2020, 189, 105124.
30. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Commun. Surv. Tutor. 2019, 21, 2671–2701.
31. Pereira, T.; Barreto, L.; Amaral, A. Network and information security challenges within Industry 4.0 paradigm. Procedia Manuf. 2017, 13, 1253–1260.
32. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4.
33. Moyne, J.; Mashiro, S.; Gross, D. Determining a security roadmap for the microelectronics industry. In Proceedings of the 2018 29th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC), Saratoga Springs, NY, USA, 30 April–3 May 2018; pp. 291–294.
34. Benias, N.; Markopoulos, A.P. A review on the readiness level and cyber-security challenges in Industry 4.0. In Proceedings of the 2017 South Eastern European Design Automation, Computer

Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Kastoria, Greece, 23–25 September 2017; pp. 76–80, ISBN 978-618-83314-0-2.

35. Hassanzadeh, A.; Modi, S.; Mulchandani, S. Towards effective security control assignment in the Industrial Internet of Things. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 795–800.
36. Autenrieth, P.; Lörcher, C.; Pfeiffer, C.; Winkens, T.; Martin, L. Current significance of IT-infrastructure enabling industry 4.0 in large companies. In Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17–20 June 2018; pp. 1–8.
37. Esposito, C.; Castiglione, A.; Martini, B.; Choo, K.-K.R. Cloud Manufacturing: Security, Privacy, and Forensic Concerns. IEEE Cloud Comput. 2016, 3, 16–22.
38. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.
39. de Lacalle, L.N.L.; Posada, J. Special issue on new Industry 4.0 advances in industrial IoT and visual computing for manufacturing processes. Appl. Sci. 2019, 9, 4323.
40. Tayyaba, S.; Khan, S.A.; Tariq, M.; Ashraf, M.W. Network security and Internet of things. In Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital; IGI Global: Hershey, PA, USA, 2020; pp. 198–238.
41. Logrippo, L. Multi-level models for data security in networks and in the Internet of things. J. Inf. Secur. Appl. 2021, 58, 102778.
42. El-Latif, A.A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E.; Elwahsh, H.; Piran, J.; Bashir, A.K.; Song, O.-Y.; Mazurczyk, W. Providing End-to-End Security Using Quantum Walks in IoT Networks. IEEE Access 2020, 8, 92687–92696.
43. Li, Y.; Sha, J.; Geng, R. Research on internal network data security monitoring method based on NB-IOT. Web Intell. 2021, 19, 191–202.
44. Batra, I.; Verma, S.; Kavita; Alazab, M. A lightweight IoT-based security framework for inventory automation using wireless sensor network. Int. J. Commun. Syst. 2020, 33, e4228.
45. Kalyani, G.; Chaudhari, S. Cross Layer Security MAC Aware Routing Protocol for IoT Networks. Wirel. Pers. Commun. 2022, 123, 935–957.
46. Ali, F.; Mathew, S. An efficient multilevel security architecture for blockchain-based IoT networks using principles of cellular automata. PeerJ Comput. Sci. 2022, 8, e989.
47. Hu, B.; Tang, W.; Xie, Q. A two-factor security authentication scheme for wireless sensor networks in IoT environments. Neurocomputing 2022, 500, 741–749.

48. Shahid, H.; Ashraf, H.; Javed, H.; Humayun, M.; Jhanjhi, N.; AlZain, M.A. Energy Optimised Security against Wormhole Attack in IoT-Based Wireless Sensor Networks. Comput. Mater. Contin. 2021, 68, 1967–1981.
49. Teng, D. Industrial Internet of Things Anti-Intrusion Detection System by Neural Network in the Context of Internet of Things for Privacy Law Security Protection. Wirel. Commun. Mob. Comput. 2022, 2022, 1–17.