WSN-IoT

Subjects: Computer Science, Information Systems

Contributor: Muhammad Zunnurain Hussain, Zurina Mohd Hanapi

The Wireless Sensor Network in the Internet of Things (WSN-IoT) has been flourishing as another global breakthrough over the past. The WSN-IoT is reforming the way we live today by spreading through all areas of life, including the dangerous demographic aging crisis and the subsequent decline of jobs. For a company to increase revenues and cost-effectiveness growth should be customer-centered and agile within an organization. WSN-IoT networks have simultaneously faced threats, such as sniffing, spoofing, and intruders. However, WSN-IoT networks are often made up of multiple embedded devices (sensors and actuators) with limited resources that are joined via various connections in a low-power and lossy manner.

Keywords: internet of things ; industrial internet of things (IIoT) ; low powered

1. Introduction

IoT has been thriving as another global innovation in the last few years. It is expected that the world's fortunes will be changed by implementing IoT in various systems over the coming years. IoT will likely revolutionize the way we live today. The Internet of Things foundation was established to improve communication and data exchange between humans and devices for massive data transfer [1]. IoT's motivation involves the association of registering gadgets, mechanical and computerized objects, humans, and machines through applications utilizing the web interface and portable applications. The IoT climate can move information through an organization without expecting human-to-human or human-to-computer correspondence [2].

IoT is becoming a significant necessity for many industrial and communication technology applications. There has been an enormous increase in IoT implementation as it has been considered to have the massive number of 50 billion devices connected to the Internet by 2020 [3]. Furthermore, IoT applications designed to assist the disabled or elderly provide ease and mobility at varying degrees of unconventionality for a reasonable price [4]. In addition, IoT adds to numerous fields, for example, agribusiness, climate, clinical areas, the educational sector, transportation, and finance.

Numerous organizations and scientific research associations are working on various aspects of the IoT. They have presented a functional outline for the IoT's impacts on the economy and the vast majority of other existing fields over the next 10 years. Cisco is the primary organization that delivers numerous IoT undertakings, which included 24 billion smart objects by 2019. It is also expected that the Huawei company will introduce 100 billion IoT associations by 2025 [5][6][7]. Every second in the world, 127 devices are linked to the Internet. By 2020, out of all electronic device use, 63% will be using IoT technology. Of all the massive, smart city commercial projects, 23% consist of IoT implementation, while by the end of 2020, 40% of all healthcare organizations were embedding IoT [8].

Via controllers and cloud management, autonomy can be generated for the self-sufficiency and decision-making of nodes [9]. There is always a wide open door for intruders or hackers to utilize IoT devices for their potential benefit via various attacks, such as Denial-of-Service (DoS) attacks, phishing emails, and other unsafe worms or Trojans [10]. The IoT layers present multiple risks such as sniffing, spoofing, eavesdropping, and intrusion. IoT utilizes hubs, sensors, and intelligent recognition gadgets to gather information. Because of the nonappearance of verification administration, unapproved access can change data integrity or even erase the stored data [11][12].

IoT systems can work under various conditions and, in most cases, have little computing capacity. Therefore, specific IoT devices can connect to many hubs, raising significant security concerns. As a result, security issues have proven to be more challenging to solve, as it is difficult to establish a nonexclusive security architecture or model [13]. The Internet has undergone remarkable changes that offer both extraordinary opportunities and significant difficulties for users; troubles emerge from unauthorized users utilizing cyberspace and exploiting its numerous weaknesses. Various cyber insights are required for the Internet to assess risks and overcome challenges [14].

The increasing proliferation of WSN devices in an actuating–communicating network has spawned the Internet of Things (IoT), in which data is seamlessly shared across platforms by fusing sensors and actuators with surroundings. Medical and environmental monitoring can be automated using these low-cost WSN devices. RPL improves the utilization of these sensors in real-world applications by assessing their performance. Low-Power and Lossy Networks (LLNs) are mainly restricted nodes with limited processing power and fluctuating energy. Most traffic patterns are multipoint-to-point or multipoint-to-multipoint rather than point-to-point. As a result, data rates are often reduced, resulting in instability [15]. Contiki is an operating system that allows RPL and lossless monitoring of Internet of Things devices. Topological node assignment is based on multi-hop transmissions and has been employed in environmental monitoring, health care, and other smart systems [16]. Routing is a popular topic in the IoT community because of the limitations imposed by these devices. In many IoT networks, the Internet Engineering Task Force's (IETF) routing protocol for low power and lossy networks (LPN) has become the norm since it was intended to effectively utilize the finite resources of IoT devices while delivering effective routing services. RPL's architecture included many but optional security methods for ensuring reliable routing. Research on the security elements of RPL's routing protocol, such as routing assaults, novel mitigation mechanisms and intrusion detection systems (IDSs), and goal functions with an eye on security, has exploded since the protocol's 2012 standardization (OFs). The impacts of RPL's security features against routing assaults have not yet been studied, which is strange. RPL's security features have not been implemented in any of the existing IoT operating systems (OSs), such as Contiki OS and TinyOS.

2. IoT-LPN Architecture and Its Applications

The Internet of Things employs low-power and lossy networks, known as Low-Power and Lossy Networks (LLN), which may impose limits on infrastructure integration. It enables devices to interact with embedded devices, such as sensors, and can connect many nodes. The traffic variety of LLN systems is also defined; they use point-to-point, point-to-multipoint, and multipoint-to-multipoint architectures. Because of the intricacy of such a network, it is critical to have a routing protocol that serves the purpose. This has been one of the researchers' primary problems. So, to achieve this goal, the IETF ROLL working group developed RPL, a protocol for LLNs. This protocol is built on a collection-based network in which nodes gather information at regular intervals and transfer it to the collection point. The entire communication architecture is built on low-power wide area networks (LPWA) using unlicensed spectrum (Sigfox, LoRa) and other LPWA technologies proposed by the 3rd Generation Partnership Project (3GPP) that works within a licensed frequency range (NB-IoT, LTE-M). At the same time, the unlicensed spectrum origins made it more challenging to meet the integration goal and increased the possibility of interference and congestion. A licensed frequency range reduces external interference and improves dependability, signal-to-interference-plus-noise ratio (SINR), and security. Similarly, getting a license for these bands comes with a high upfront cost and a regular renewal price. The rise in cost will inevitably be passed on to subscribers, raising capital expenditures for deployment and ongoing operational expenses.

Software-defined networking (SDN) architectural technology increases network performance and monitoring [17][18]. However, the network system is divided into device management, the Internet of Everything (IoE) gateway, and intelligent LPWA with the help of AI and deep learning. IoE services provide cellular communication in the licensed and unlicensed spectrum. Similarly, AI is responsible for smart wireless communication technology using smart applications and IoE services. Some typical IoT applications developed with the help of LPWA are the smart city, track and trace, and smart building applications.

3. IoT-LPN Protocols

Several routing protocols have been developed to improve the efficiency and functionality of networks in IoT systems. Low-powered protocols have been prevalent in the demand for low-powered IoT frameworks as they are efficient and require fewer resources, making them practical and providing many benefits. GeoRank aims to improve P2P functionality and minimize the number of control messages needed, but it reduces scalability and requires static nodes or GPS-enabled devices. Further, the protocols are mapped with the routing solutions they present, which are P2P support, multicast communication, mobile node support, Quality of Service QoS, and energy efficiency. Energy-efficient region-based RPL (ER-RPL) is designed to prevent the network from flooding with peer-to-peer (P2P) route-finding packets, resulting in energy savings and an increase in the P2P packet delivery ratio. P2P-RPL allows for the construction of alternative P2P routes for application routing needs, but it increases the overheads and energy consumption of the network. Bidirectional multicast RPL forwarding (BMRF) improves both upstream and downstream multicast data forwarding. Still, it has a slight increase in memory consumption and can have low productivity due to end-to-end latency and incorrect parameter settings. Stateless Multicast RPL Forwarding SMRF improves RPL's multicast data forwarding and reduces energy waste but only allows for downward multicast broadcasting and can have high end-to-end latency.

mRPL provides quick and reliable mobility support in RPL but increases the length of control messages and the number of control messages sent and received. Backpressure RPL (BRPL) aims to improve RPL's performance in large-scale networks, but it requires a large amount of memory and has a high end-to-end latency.

4. IoT-LPN Research Challenges

Similarly, most LPWANs are confined to star topologies. In contrast, cellular-based networks (EC-GSM-IoT, NB-IoT, LTE Cat. M1, 5G) depend on wired infrastructure to integrate networks and cover wider regions. So, the improper infrastructure hampers applications such as the agriculture IoT [19]. The scalability of short-range and cellular wireless networks is the subject of current research. Offloading (from the licensed to the unlicensed spectrum), common in cellular-based technologies, is impractical for LPWANs operating in the unlicensed spectrum. To overcome the scalability issues, there is a need to approach some other strategies, such as adaptive data rate MAC protocols, the adaptation of spectrum-efficient modulation techniques, and LPWAN channel diversity exploration. Another significant issue is the collection of LPWAN-relevant data regarding methodologies and performances. Because the data of popular LPWANs (LoRaWAN, SigFox, and NB-IoT) is easily accessible, gathering the data for others is complicated due to fewer references. Nowadays, LPWANs are widespread and there is more demand among users to develop new applications because of the discovery of new methods applicable to their personal lives and business operations.

It is understood that security and privacy are the primary concerns in all fields. However, there has been little emphasis on LPWAN's security in general. Unauthorized access can easily breach the security of a smart home controller. Using unauthorized access, attackers can steal information and completely control home appliances, causing inconvenience to their users.

Similarly, unauthorized access to smart cities, agriculture, and inter-vehicle communication can cause death and environmental harm. So there is a need for adequate security to authenticate the user or owner efficiently; otherwise, LPWANs are not viable for commercial purposes [20]. Moreover, the essential components of security related to WSN-IoT are discussed in Section 4. These components are considered necessary before implementing any WSN-IoT application; otherwise, it will be vulnerable.

5. Security Objectives of WSN-IOT

WSN-IoT's security requirements are the essential characteristics necessary to be implemented to fulfill network security requirements. It consists of various preventive measures for the smooth functioning of the IoT framework [4][21][22][23][24][25][26].

5.1. Availability

The nature of keeping the service accessible to clients is accessibility. The goal of accessibility is to provide clients with the ability to obtain services at any time and from any location. It is critical to keep assets regularly available to clients and the organization. Consequently, all clients must be confirmed to combat assaults and risks to the organization. Accessibility may help to avoid blockage circumstances such as framework conflicts and organizational blockages that disrupt the information flow.

5.2. Accountability

Accountability is one of the WSN-IoT framework's basic properties, but it cannot preempt network attack risks and WSN-IoT vulnerabilities. However, rationing and supporting other security criteria such as data integrity and privacy are imperative. They are utilized to follow any node (device) that sends and receives information to notice and distinguish any obscure activities by providing guidelines for the device, clients, and their actions.

5.3. Confidentiality and Privacy

Confidentiality is otherwise known as privacy To fulfill the security requirements, it is implemented to prevent unauthorized clients from obtaining information. Confidentiality gives recognizable proof of verification and authorization for any sensitive item in the IoT network. Numerous security modules ensure the security of information. Maintaining data secrecy is a critical security requirement as it is vital to keep the framework intruder-proof. Privacy guarantees authorized users' private data and preempts intruders from accessing network services or stealing any data. Privacy has to be implemented at many levels. Privacy for devices is necessary to maintain physical and data confidentiality, as a network can be exposed to data intrusion. Privacy during data transmission within IoT devices preserves sensitive information. Privacy is

crucial during the processing and storing of data, as it is most vulnerable at this point. Privacy of location is intended to prevent the disclosure of the geographical position of IoT devices from intruders.

5.4. Auditing

Auditing is essential; without it, the framework's criteria for meeting security requirements will not be accomplished. It is used to recognize the security shortcomings of WSN-IoT. Auditing is entirely related to accountability, yet it depends on assessing the framework and its services. Auditing measures how well the WSN-IoT framework meets its network performance criteria and components.

6.5. Integrity

Integrity is one security idea that empowers legitimate and authorized access to modify data according to requirements under limited conditions. Integrity can forestall inner attacks, the most hazardous issue in the network framework, as all users must be validated and authorized with access rights. Notwithstanding, cybercriminals may change information during network communication. Integrity may preempt outside attacks to get to or alter sensitive information.

5.6. Access Control

Network access control is verified by an authorized network administrator for the smooth management of user access. It gives clients/users explicit roles or verified admittance to utilize network assets to view, alter, or modify data. Access control offers certain rights to legitimate users to perform precise work.

5.7. Authentication and Authorization

Authentication is the user's verification, the primary security necessity, as it recognizes users as validated clients utilizing security frameworks such as cryptography algorithms. After authentication, authorization plays a role in the approval of authentic users to use network services.

6. Security Issues and Challenges in WSN-IOT

6.1. Data Confidentiality

In the field of WSN-IoT and network protection, data secrecy is a critical concern. The client has access to the details and the system management in WSN-IoT frameworks. The IoT device should check that the user or machine has been granted access to the system [27]. Approval determines whether a person or device can receive assistance after presenting distinguishing evidence. Access management restricts property access by granting or refusing permission based on a series of laws. Creating a secure connection between devices and services necessitates approval and access control. The main point is creating a specific relationship between other devices and administrations, which requires support and access control. The most critical problem in this situation is making access management regulations easy to develop and understand. This is a vital issue in the Internet of Things; many clients, objects, and devices must verify each other through trustworthy administrations to gain system access. The problem is to find a solution for safely dealing with the client's personality, items, and gadgets [28][29].

6.2. Privacy

Privacy and confidentiality are significant issues in WSN-IoT gadgets and frameworks under the IoT systems' universal character. Entities are linked, and information is conveyed and exchanged via the Internet, delivering client protection and causing various risks to sensitive information in many ways. So that the exploration issues are satisfied, knowledge acquisition security is just as important as information sharing security. Information protection is one of the primary uncertainties in the WSN-IoT because of the high chance of security vulnerabilities, such as sniffing and spoofing, unapproved access, data altering, and forgery with the unapproved altering of IoT nodes [30]. An aggressor can exploit numerous WSN-IoT administrations and applications to store sensitive and personal data, and if they are exposed, unstable and sensitive data can be exposed to outsiders [27][31].

6.3. Trust Management

In WSN-IoT frameworks, there is a consequence of regional conventions, resources, and limits of distinctive devices, which is a considerable assessment of IoT trust management. Trust is a significant part of WSN-IoT security, data security, administration, applications, and client protection. Trust is a fundamental component of communications among WSN-IoT devices to trade and manage information. IoT layers have a unique assortment of gadgets. Every gadget

creates an enormous amount of information vulnerable to various assaults, dangers, and issues. These issues and attacks have the potential to spread across all IoT layers. As a result, the accuracy of information and administration will be reduced [30][32].

Trust management in IoT ought to accomplish the accompanying objectives of having faith in IoT nodes and choices to help one another. It should moderate client security, information transmission, and trust correspondence, as indicated by the IoT system's strategy. It should increase the superiority of IoT services, framework security, and reliability [33][34][35]. Furthermore, clients should not be aware of it.

6.4. Vulnerabilities

Vulnerabilities are flaws, and flaws in a system or plan that allow attackers to run commands, access unapproved data, and trigger DoS. In WSN-IoT implementations, bugs may be identified in several locations. They can be weaknesses in the client's devices and flaws in the system's hardware, code, or techniques used in the methods [36]. Hardware and software are the two fundamental components of IoT architecture. Both have configuration flaws daily. Hardware loopholes are challenging to detect and repair, regardless of whether the vulnerabilities were identified due to equipment similarities and interoperability, or the effort required to overcome them [13]. They can be found in working systems, application programming, and control programs, such as communications conventions and software changes. A significant cause of exposure is human error. The consequences of not understanding the necessities of teamwork, requirement engineering, testing and validation, security assessment, data integrity, and privacy can cause the framework to fail [37].

6.5. Security

Physical, network, and data protection are significant issues in WS-IoT frameworks. The growth in the number of connected devices on communication networks in the IoT [38] leads to increased security risks and new security challenges. Protection risks are acquired by any node that connects to the Internet, whether it is a limited or smart device [39]. On the Internet of Things, you can find almost any security issue. As a result, a few primary security criteria in the IoT, such as acceptance, confirmation, classification, confidence, and information security, should be considered.

Consequently, things should be safely associated with their assigned networks, flexibly controlled, authenticated, and authorized [40]. Physical security tampering, stealing, and attacks are performed on IoT devices. The attacker can grab and steal a node or exchange it with a malicious node, causing harm to the whole network; moreover, the intruder can break the node or steal valuable or peculiar information that could be used against the system [41]. Maintaining a secure network means stopping intruders from finding their way into the system and causing severe damage by sending malware, sniffing, spoofing, stealing sensitive data, man-in-the-middle eavesdropping, or performing DoS attacks. Outsiders or employees within the organization can be intruders. Data security entails ensuring data integrity and privacy while data is transferred within the framework. Security is a method of protecting information from tyrannical forces or unauthorized access. IoT security depends heavily on information security, also known as computer security. [42].

6.6. Interoperability

A fractured landscape hampers users' value with patented IoT technical execution. Even if complete interoperability across goods and services is not always possible, consumers cannot like purchasing products and services that lack versatility and are subject to distributor lock-in [43]. Poorly designed WSN-IoT devices can negatively impact the networking resources to which they are linked. Another significant factor is cryptography, which has been used for years to protect against security vulnerabilities in several applications. A single protection application cannot have a suitable defense mechanism against attacks [44]. As a result, various levels of security are required to counteract WSN-IoT authentication risks. Hacks could be avoided by designing more sophisticated security features and incorporating them into devices. This evasion occurs because consumers purchase goods with good security features to guard against vulnerabilities. Any of the steps suggested to guarantee that the IoT is safe are cyber-security mechanisms [45].

6.7. Identification, Authentication, and Authorization

Nodes are the IoT building blocks that need to be defined in the network or physically. IoT networks cover a large area to track the transmission between devices and acquire access to the entire network. The total naming layout of nodes is unsafe without data consistency [46]. DNS cache positioning assaults may wreak havoc on the network's overall performance. For each target to be uniquely identified, node identification is necessary. The false node should be detected efficiently since each mark indicates a potential attack location. The network must be defended against physical or logical attacks on devices and their data. Authentication requires checking the identity of the nodes [47]. Undeniably, if contact

with the correct node is not ensured, the secrecy and fairness of the messages exchanged cannot be guaranteed. An attacker can access the network and insert erroneous statements if the authentication is poorly handled. It is challenging to ensure authentication because of the wireless media's existence and the nature of sensor networks. Authentication involves confirming that you are who you claim to be. This is commonly achieved using an authentication method based on a username and password [48]. This scheme, though, is not safe enough. Passwords typically need to be updated regularly, and unattended computers should not be used. Authentication also requires the authentication method for both the sender and the recipient to validate the messages' origin [49].

6.8. Attacks

"The IoT frameworks hold a vast volume of information; the network layer is particularly vulnerable to attacks, creating much network congestion." The network's data integrity and authentication are critical security problems [50]. A significant problem is an attack by hackers and rogue nodes that damage the network's computers. The current security restrictions applied to IoT render them susceptible to attacks. Based on the particular design and features of the WSNs, these attacks usually follow new tactics [51]. Indeed, in the Open System Interconnection (OSI) model, attacks can be characterized according to the targeted protocol layer. Another method of grouping classifies assaults depending on the existence of the offender.

Passive threats are confined exclusively to the study, capture, and data snooping of traffic. Active attacks, however, usually exploit the data by disrupting the connection between the nodes and affecting the nodes' availability, so attacks can also be carried out [52]. On the other hand, internal attacks are initiated by valid network nodes that function against their requirements.

References

1. Evans, D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. 2011. Available online: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL (accessed on 11 December 2022).
2. Lakshmi, I. The Internet of Things (IoT) and Cyber Security: Vulnerabilities, Threats, Intruders and Attacks. IOSR J. Comput. Eng. (IOSR-JCE) 2017, 19, 85–94.
3. Libelium. 50 Sensor Applications for a Smarter World. 2020. Available online: https://www.libelium.com/libeliumworld/top-50-iot-sensor-applications-ranking (accessed on 11 December 2022).
4. Jimenez, J.; Koster, M.; Tschofenig, H. IPSO smart objects. In a Position paper for the IOT Semantic Interoperability Workshop, 2016.
5. Dragomir, D.; Gheorghe, L.; Costea, S.; Radovici, A. A survey on secure communication protocols for IoT systems. In Proceedings of the 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, 26–30 September 2016; pp. 47–62.
6. Pishva, D. Internet of Things: Security and privacy issues and possible solution. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 19–22 February 2017; pp. 797–808.
7. Huawei. Tap into New Growth with Intelligent Connectivity. 2018. Available online: https://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180716 (accessed on 11 December 2022).
8. Vega, M. Internet of things statistics facts & predictions . Retrieved Novemb. 2020, 30, 2020.
9. Tan, X.; Su, S.; Huang, Z.; Guo, X.; Zuo, Z.; Sun, X.; Li, L. Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm. Sensors 2019, 19, 203.
10. Ostadal, R.; Matyas, V.; Svenda, P.; Nemec, L. Crowdsourced security reconstitution for wireless sensor networks: Secrecy amplification. Sensors 2019, 19, 5041.
11. Gendreau, A.A.; Moorman, M. Survey of intrusion detection systems towards an end-to-end secure internet of things. In Proceedings of the 2016 IEEE 4th International Conference on the Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 84–90.
12. Lee, C.-C. Security and privacy in wireless sensor networks: Advances and challenges. Sensors 2020, 20, 744.
13. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Comput. Netw. 2015, 76, 146–164.

14. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, A.V. Security and privacy for cloud-based IoT: Challenges. IEEE Commun. Mag. 2017, 55, 26–33.
15. Alansari, Z.; Prasanth, A.; Belgaum, M. A comparison analysis of fault detection algorithms in wireless sensor networks. In Proceedings of the 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 18–20 November 2018; pp. 1–6.
16. Lee, T.H.; Xie, X.S.; Chang, L. RSSI-based IPv6 routing metrics for RPL in low-power and lossy networks. In Proceedings of the 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), San Diego, CA, USA, 5–8 October 2014; pp. 1714–1719.
17. Priyadarsini, M.; Bera, P. Software-defined networking architecture, traffic management, security, and placement: A survey. Comput. Netw. 2021, 192, 108047.
18. Radel, J. Organizational Change and Industry 4.0 (id4). A perspective on possible future challenges for Human Resources Management. Ind. Von Morgen 2017, 5, 32–39.
19. FarmBeats: AI, Edge & IoT for Agriculture. 2015. Available online: https://www.microsoft.com/en-us/research/project/farmbeats-iot-agriculture/ (accessed on 11 December 2022).
20. Buurman, B.; Kamruzzaman, J.; Karmakar, G.; Islam, S. Low-power wide-area networks: Design goals, architecture, suitability to use cases and research challenge. IEEE Access 2020, 8, 17179–17220.
21. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication protocols for the internet of things: A comprehensive survey. Secur. Commun. Networks 2017, 2017, 6562953.
22. Iqbal, M.A.; Olaleye, O.G.; Bayoumi, M.A. A review on internet of things (IoT): Security and privacy requirements and the solution approach. Glob. J. Comput. Sci. Technol. 2016, 16, 1–9.
23. Ravindran, R.; Yomas, J.; Sebastian, E.J. IoT: A review on security issues and measures. Int. J. Eng. Sci. Technol. 2015, 5, 348–351.
24. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for Internet of Things. J. Netw. Comput. Appl. 2014, 42, 120–134.
25. Sun, Y.; Apostolaki, M.; Birge-Lee, H.; Vanbever, L.; Rexford, J.; Chiang, M.; Mittal, P. Mittal Securing internet applications from routing attacks. Commun. ACM 2021, 64, 86–96.
26. Rajasekar, V.; Rajkumar, S. A Study on Impact of DIS flooding Attack on RPL-based 6LowPAN Network. Microprocess. Microsyst. 2022, 94, 104675.
27. Dalipi, F.; Yayilgan, S.Y. Security and privacy considerations for iot application on smart grids: Survey and research challenges. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 63–68.
28. Fink, G.A.; Zarzhitsky, D.V.; Carroll, T.E.; Farquhar, E.D. Security and privacy grand challenges for the Internet of Things. In Proceedings of the 2015 International Conference on Collaboration Technologies and Systems (CTS), Atlanta, GA, USA, 1–5 June 2015; pp. 27–34.
29. Henze, M.; Hermerschmidt, L.; Kerpen, D.; Häußling, R.; Rumpe, B.; Wehrle, K. A comprehensive approach to privacy in the cloud-based Internet of Things. Future Gener. Comput. Syst. 2016, 56, 701–718.
30. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In Proceedings of the 2015 IEEE World Congress on Services, New York, NY, USA, 27 June–2 July 2015; pp. 21–28.
31. Ling, Z.; Liu, K.; Xu, Y.; Jin, Y.; Fu, X. An end-to-end view of iot security and privacy. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7.
32. Sicari, S.; Rizzardi, A.; Miorandi, D.; Coen-Porisini, A. REATO: REActing TO Denial of Service attacks in the Internet of Things. Comput. Netw. 2018, 137, 37–48.
33. Abomhara, M. Department of Information and Communication Technology, University of Agder, Norway, GM Køien, and Department of Information and Communication Technology, University of Agder, Norway, Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. J. Cyber Secur. Mobil. 2015, 4, 65–88.
34. 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.
35. Zhou, J.; Dong, X.; Cao, Z.; Vasilakos, A.V. Secure and privacy-preserving protocol for cloud-based vehicular DTNs. IEEE Trans. Inf. Forensics Secur. 2015, 10, 1299–1314.
36. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the internet of things: A survey of existing protocols and open research issues. IEEE Commun. Surv. Tutor. 2015, 17, 1294–1312.

37. Ranjan, A.K.; Somani, G. Access control and authentication in the internet of things environment. In Connectivity Frame works for Smart Devices; Springer: Berlin/Heidelberg, Germany, 2016; pp. 283–305.
38. Iotforall. The Role of IoT and Industry 4.0 in Creating Digital Factories of Tomorrow. 2022. Available online: https://www. iotforall.com/the-role-of-iot-and-industry-4-0-in-creating-digital-factories-of-tomorrow (accessed on 11 December 2022).
39. Zaldivar, D.; Lo, A.T.; Muheidat, F. Investigating the security threats on networked medical devices. In Proceedings of th e 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 Ja nuary 2020; pp. 0488–0493.
40. Lo'ai, A.T.; Somani, T.F. More secure Internet of Things using robust encryption algorithms against side-channel attack s. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCS A), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.
41. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet archit ecture. Future Internet 2017, 9, 27.
42. Dabbagh, M.; Rayes, A. Internet of things security and privacy. In The Internet of Things from Hype to Reality; Springer: Berlin/Heidelberg, Germany, 2019; pp. 211–238.
43. Perera, C.; Ranjan, R.; Wang, L.; Khan, S.U.; Zomaya, A.Y. Big data privacy in the internet of things era. IT Prof. 2015, 17, 32–39.
44. Ziegeldorf, J.H.; Morchon, O.G.; Wehrle, K. Privacy in the Internet of Things: Threats and challenges. Secur. Commun. Netw. 2014, 7, 2728–2742.
45. Vasilomanolakis, E.; Daubert, J.; Luthra, M.; Gazis, V.; Wiesmaier, A.; Kikiras, P. On the security and privacy of internet of things architectures and systems. In Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT), Vienna, Austria, 21–25 September 2015; pp. 49–57.
46. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating critical security issues of the IoT world: Present and future challe nges. IEEE Internet Things J. 2017, 5, 2483–2495.
47. Gai, K.; Choo, K.-K.R.; Qiu, M.; Zhu, L. Privacy-preserving content-oriented wireless communication in internet-of-thing s. IEEE Internet Things J. 2018, 5, 3059–3067.
48. Glissa, G.; Rachedi, A.; Meddeb, A. A secure routing protocol based on RPL for Internet of Things. In Proceedings of th e 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–7.
49. Boubiche, D.E.; Athmani, S.; Boubiche, S.; Toral-Cruz, H. Cybersecurity issues in wireless sensor networks: Current ch allenges and solutions. Wirel. Pers. Commun. 2021, 117, 177–213.
50. Safdar, Z.; Farid, S.; Pasha, M.; Safdar, K. A security model for iot based systems. Tech. J. 2017, 22.
51. Saibabu, G.; Jain, A.; Sharma, V. Security issues and challenges in IoT routing over wireless communication. Int. J. Inn ov. Technol. Explor. Eng. 2020, 9, 1572–1580.
52. Wittenberg, C. Cause the trending Industry 4.0 in the automated industry to new requirements on user interfaces? In Pr oceedings of the International Conference on Human-Computer Interaction, Bamberg, Germany, 14–18 September 20 15; pp. 238–245.