Security and Privacy of Internet of Things: A Review of Challenges and Solutions

Yujing Lu

Shijiazhuang University of Applied Technology, Shijiazhuang, China
E-mail: luyujinglj@163.com

Received 07 May 2023; Accepted 01 July 2023;
Publication 17 November 2023

Abstract

The Internet of Things (IoT) is a global and comprehensive network that monitors and controls the physical world by collecting, processing, and analysing data derived from IoT devices. Globally, the IoT is emerging as a trend bringing intelligence and automation to a variety of application domains, presenting both opportunities and security challenges. It is used in various fields, including medical care, smart grids, home automation, smart cities, etc. As the number of devices connected to the IoT increases, there is an increased risk of cyber-attacks, data breaches, and other malicious activities. This means that it is essential to have secure protocols and encryption methods in place to protect the data being exchanged. This paper identifies and synthesizes security issues related to the IoT. Security threats across different layers of the IoT architecture are discussed first, followed by identifying prevalent security and privacy issues. A discussion is also provided on security countermeasures.

Keywords: Internet of Things, security, future development, review.

Journal of Cyber Security and Mobility, Vol. 12_6, 813–844.
doi: 10.13052/jcsm2245-1439.1261

1 Introduction

In recent years, the advancement of various technology areas, such as broadband internet access, wireless communications, embedded computing, and automated identification and tracking, has resulted in intelligent items becoming part of our everyday lives. The Internet of Things (IoT) refers to the integration of the Internet with real-world items present in various areas, including environmental monitoring, smart homes, industrial processes, and health monitoring [1]. Blockchain, humanitarian logistics, cloud computing [2], machine learning [3–5], and artificial intelligence [6, 7] are pivotal in the IoT ecosystem for boosting efficiency, security, and innovation. Blockchain ensures secure and transparent transactions among IoT devices [8], while humanitarian logistics utilizes IoT capabilities for coordinated aid delivery during emergencies [9]. Cloud computing provides scalable storage and computing resources for seamless connectivity and analysis of IoT-generated data. Machine learning and artificial intelligence enable intelligent decision-making, predictive analytics, and automation in the IoT ecosystem, improving operational efficiency across a broad range of sectors, such as healthcare, transportation, agriculture, and smart cities [10–12]. In the upcoming years, it is expected to play a fundamental role in the Information and Communications Technology (ICT) industry. By leveraging the power of IoT technology, businesses can gain a competitive advantage in the ICT industry, experiencing greater operational efficiency, enhanced user experiences, and improved decision-making [13].

Although IoT offers better opportunities for connecting the advanced and physical worlds, cybersecurity threats are also on the rise. There is a growing concern that the digital threat is not limited to large business networks or data, where organizations have tended to concentrate their cyber security efforts. Programmers are also looking for ways to attack devices outside conventional perimeters. Due to the precipitate growth in the number of IoT devices and the wide range of capabilities, they can provide, there is an increase in expected vulnerabilities [14]. As IoT devices become increasingly common and accessible, they become attractive targets for malicious actors. These devices often lack the same security level found in more traditional computing systems, leaving them vulnerable to attack. Additionally, these devices are often connected to large networks, making them potential entry points for attackers [15].

Recognizing security risks and developing solutions in IoT-enabled environments takes extra energy and time. Since all objects exchange information

over the Internet, the IoT has exposed a number of security risks. There are also concerns about end-user privacy. IoT development has been slowed for a variety of reasons, mainly due to a lack of technological advancements and the existence of a security challenge. In this way, with all its advanced information exchange capabilities, the IoT is a flawed concept in terms of security. Therefore, it is better to take appropriate steps in its initial phases, i.e., creating security, before further development for widespread and effective acceptance. Security and privacy are key issues for IoT applications. Following the growth of the IoT nationwide and its impact on people's lifestyles, the need for privacy and security has multiplied and made it a major challenge [16]. This research has examined the application areas of IoT Security in the first stage. These applications are categorized into 12 groups. In the second part, the aim is to identify the approaches adopted in IoT security upgrades. The rest of the paper is organized in the following manner. Section 2 presents a background of IoT and its security and privacy. Section 3 contains a systematized taxonomy of IoT security applications. IoT privacy and security solutions and challenges are highlighted in Sections 4 and 5, respectively. Finally, Section 6 brings this research to a conclusion.

2 Backgrounds

The IoT has evolved into an infrastructure that facilitates interconnection between physical sensors, smartphones, and smart buildings. This electronic device exchange information wirelessly or through wired channels. By harnessing the power of the IoT, businesses are able to gain valuable insights into customer behavior and usage patterns, allowing them to make more informed decisions about their operations.

2.1 IoT Architecture

IoT does not simply refer to an internet-connected device but is the technology that enables a system to sense, react, and respond to the world without any human intervention. By leveraging sensors, actuators, and other technologies, IoT can collect data, process it, and then take action based on the conclusions. This, in turn, creates a feedback loop that continuously learns and improves its response over time, allowing it to autonomously respond to changes in its environment [17]. As shown in Figure 1, the IoT architecture consists of several stages that work together to collect, transform, and process data. The first stage involves collecting data from the environment

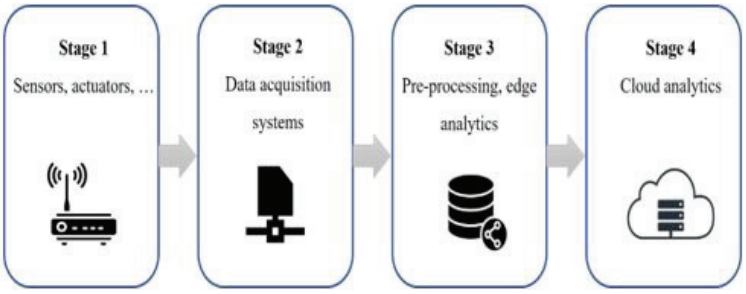


Figure 1 Stages of IoT working.

and transforming it into usable information. Smartphones, equipped with sensors, play a crucial role in this process. These sensors detect the earth's gravitational pull, allowing users to adjust the screen orientation based on the device's position.

By collecting and transforming data, smartphones provide users with a seamless and intuitive experience, enabling them to interact with their environment more efficiently. Actuators are devices that can generate data by affecting physical reality. By incorporating actuators, smartphones have become invaluable tools in our daily lives, empowering us to interact with the world more efficiently, reliably, and intuitively. The second stage of the IoT architecture involves an internet gateway. This system aggregates and converts data received from sensors into a digital format. It enables machines to intelligently analyze real-time data by using data acquisition devices. These devices capture signals and environmental conditions, making them essential in industrial, commercial, and scientific equipment. In the third stage, Edge IoT, prepared data is transferred to the IT world at high speeds. This stage facilitates quick data processing and offers additional flexibility. The data is transferred to cloud platforms where further analysis and processing take place. The fourth and final stage of the IoT architecture is the cloud and data center. This is where the main processes occur. The data center and cloud enhance the security and computational power of the IT system, enabling robust data analysis and storage.

2.2 IoT Challenges

IoT devices use embedded sensors and actuators to collect, process, and exchange data with other connected devices, allowing them to interact with each other and the environment. This enables them to be used in a wide range of applications, ranging from healthcare and home automation to

Table 1 IoT-related challenges

IoT Challenges	Advantages	Restrictions
Scalability	Adding new devices	Network capacity
Big data	Using big data analysis to gain useful insights	High latency, redundancy, and other benefits of data centralization
Security and privacy	Enabling cutting-edge apps that make use of sensitive data	Inspection of personal information

transport and industrial automation. As a result, accurate authentication and classification techniques and sufficient solutions to ensure confidentiality and integrity are required [18]. Despite several research efforts on IoT technology, the technological limitations stated in Table 1 remain. According to Table 1, the nature of the IoT, the growth of IoT, privacy, and security have grown in various fields. As the data collected by IoT devices becomes more valuable, the demand for secure protocols for data sharing and storage grows. IoT technology also allows for the development of new applications, such as automated home systems and healthcare, which further increases its use. Additionally, privacy and security concerns have become a major issue, leading to an increased focus on developing secure protocols for data sharing and storage. To ensure that data is kept safe from external threats, network administrators must implement strong authentication and encryption protocols. Additionally, they must guarantee that all devices connected to the IoT network are securely updated with the latest firmware and security patches to prevent malicious actors from exploiting known vulnerabilities. In order to ensure network security, tools, and protocols should be readily available, as well as, if possible, hardware and software installed [19].

2.3 Security in the IoT

The limitations and ubiquity of IoT networks make them susceptible to diverse attacks. IoT networks are typically designed with limited processing and storage capabilities, potentially making them vulnerable to manipulation or disruption. Additionally, the sheer number of devices connected to these networks creates a large attack surface for malicious actors to exploit. These issues arise due to the specific characteristics of security and the way in which it is implemented in IoT networks. Security concerns in the IoT mainly arise from the following factors:

- IoT is a multifaceted paradigm encompassing a wide range of applications and requirements. A broad implementation of IoT illustrates the

enormous complexity of such systems. As the number of connected devices increases exponentially, it becomes increasingly difficult to manage the data flow and interactions between them. This complexity can cause a number of issues, such as the need for additional hardware and software for security, the need for energy-efficient solutions, and the need for scalability.

- The IoT technology is extremely diverse in terms of protocols, platforms, and devices, consists mostly of limited resources, is built with lossy connectivity, and is not standardized. The characteristics of these IoT systems can be considered bottlenecks, preventing the implementation of effective and general security measures [19].
- IoT devices can be configured to automatically adapt to their environment. An effective IoT security solution that provides comprehensive protection for each device is required in these situations. Moreover, a security policy that is regularly updated and enforced should be implemented to ensure the ongoing protection of these IoT devices.
- Since most IoT physical items are ubiquitous and physically accessible, the implementation of IoT systems may enhance physical assaults. Malicious actors could use the data gathered by IoT devices to gain access to physical locations and assets, as well as to manipulate the environment for their own gain. This could lead to real-world security risks, such as the potential for physical harm.

2.4 A Taxonomy of Security in the IoT

IoT security has become a major concern in recent years. A corrupted Internet-connected item poses a threat to the security of IoT devices and threatens the entire Internet. As IoT comprises a variety of devices and equipment, ranging from small advanced embedded chips to large high-end servers, security issues must be addressed at several levels. IoT security problems can be classified as follows.

- Issues with low-level security
- Issues with intermediate-level security
- Issues with high-level security

Security and privacy are critical aspects of IoT development. The dynamic nature of IoT networks poses a variety of vulnerabilities for traditional IoT security and privacy solutions, but emerging technologies address other concerns. Table 2 illustrates these difficulties.

Table 2 Current IoT security challenges

Layer	Security Challenges
Perception	Identifying the defective sensor node The key management systems and cryptography algorithms that will be used The data and the sender's anonymity Vulnerabilities in electronic gadgets
Network	Communication with IPv6 nodes via IPSec is enabled.
Application	Computer networks that can be configured

Table 3 Taxonomy of IoT security applications

Areas	Studies
Banking system	[20, 21]
Supply chain	[22–28]
Smart home	[29–38]
Agriculture	[39–49]
Smart grid	[50–57]
Smart cities	[58–69]
Industry	[70–72]
Education	[73–78]
Military	[79–88]
Business	[89–94]
Transportation	[95–110]
Healthcare	[111–148]

3 Application of IoT Security

Security has been a constant concern for industries when it comes to IoT. This study presents a survey of IoT security research and its application domains. Publications are categorized according to application areas into 12 categories. Table 3 summarizes the findings of this study.

3.1 IoT Security and Transportation

Smart transportation systems benefit from IoT to optimize transportation resources and enhance traffic management. In the past few years, a wide range of IoT-enabled smart transportation systems applications has been developed at scale. Data collected from millions of vehicles are used to establish a data-driven traffic network called the Internet of Vehicles (IoV). IoT drives smart transportation to become increasingly embedded with Cyber-Physical systems (CPSs), which are supported by sensor networks and open network

technologies. Due to the decentralization, complexity, and heterogeneity of IoT-based systems, CPS-embedded intelligent transportation presents a number of issues relating to 5G network connectivity and cybersecurity. First, owing to the real-time transport of IoT traffic and the need for quick responses from smart applications, wireless network communication capacity and security are of the utmost importance for IoT-enabled transportation systems. The current IoT-based transportation systems suffer from high communication costs and low bandwidth. In addition, embedded nodes do not necessarily possess physical security and are susceptible to a variety of risks. Further, device-to-device contacts enable IoT objects to exchange data independently. Data generated by devices can improve the performance of a scheme by providing useful domain knowledge. However, the decentralization, complexity, and heterogeneity of IoT-enabled transportation systems make swapping data between them challenging. Third, transportation solutions powered by IoT generate an enormous amount of data. The efficient utilization of these data can facilitate the monitoring of physical traffic conditions and enhance the efficiency of transportation systems. Due to data explosions within transportation systems, conventional security procedures are not applicable in any IoT environment because of the limited capabilities of nodes in terms of memory and processing power. Cyber-insecurity issues caused by such data explosions also pose a threat to system security because of the possibility that data will leak or be breached.

3.2 IoT Security and Healthcare

The Internet of Medical Things (IoMT) encompasses various applications that benefit the healthcare sector, including wearable medical devices, RFID tags, and implantable medical devices. The advent of 5G telecommunication networks and the implementation of IPv6 addresses play a vital role in enabling and enhancing the capabilities of these medical devices, ultimately contributing to the extension of human life expectancy. The deployment of 5G networks offers several advantages for medical devices within the IoMT ecosystem. One key benefit is the significantly increased data transfer speeds and reduced latency, enabling real-time communication and faster transmission of medical data. This is particularly important in healthcare scenarios where instant response and timely access to patient information are critical. The low latency of 5G allows medical devices to provide swift and accurate feedback, enhancing healthcare services' overall efficiency and effectiveness.

Furthermore, the high network capacity and reliability of 5G enable the seamless connectivity of a vast number of medical devices simultaneously. This is crucial in healthcare environments where numerous devices need to communicate with each other and with central systems without experiencing congestion or performance degradation. IPv6 addresses, with their vast address space, are instrumental in accommodating the growing number of medical devices in the IoMT landscape. The expanded address pool ensures that each device can have a unique identifier, enabling efficient communication and management of these devices within the network. IPv6 also provides built-in security features, such as IPsec, which can help protect the transmission of sensitive medical data and mitigate security risks. However, it is important to note that the utilization of IoMT devices introduces various security challenges. The transmission of sensor data between IoT devices can be vulnerable to security risks such as denial of power attacks, device cloning, message tampering, hijacking, and eavesdropping. As IoMT devices often have limitations in terms of processing power, memory, and battery capacity, ensuring both interoperability and security becomes a critical concern.

To address these challenges, robust security measures, including encryption, authentication protocols, and secure data transmission methods, need to be implemented. Additionally, comprehensive risk assessments and privacy safeguards should be in place to protect patient's sensitive information and ensure regulatory compliance. In summary, the combination of 5G telecommunication networks and IPv6 addresses is pivotal in enabling medical devices within the IoMT ecosystem. These technologies enhance data transfer speeds, reduce latency, and provide the necessary scalability to accommodate a growing number of devices. However, it is essential to address the security challenges associated with IoMT to safeguard patient data and ensure the reliable and secure operation of medical devices.

3.3 IoT Security and Business

Even though some early IoT investors have succeeded, most companies are still pondering whether they should join the IoT since the ecosystem is unstructured, innovations are immature, and objects are diverse. These characteristics prevent an effective business model from being developed. Due to these characteristics, a variety of proprietary platforms and proprietary end-to-end IoT solutions are used, while the unstructured ecosystem creates doubts for investors because the scenario is too chaotic. Interoperability and security issues must be addressed thoroughly to achieve end-to-end IoT security. A solid business model for IoT could be built using these solutions.

3.4 IoT Security and Military

The growing trend of IoT in the military has become crucial for achieving military objectives. However, it also brings with it new security challenges. The increased connectivity and integration of IoT technologies within the military landscape expand the attack surfaces across various devices and systems. While in the past, cyber-attacks were primarily focused on PCs, devices connected to the Internet, and smartphones, the emergence of IoT devices has added another layer of security threats alongside the advantages they offer. Furthermore, the military domain has become a prime target for hackers. Regardless of the physical distance between networks, cyber-attacks have become inevitable. Consequently, a strong argument exists for prioritizing cyber-attack protection within military operations. Traditional security solutions, such as firewalls and cryptographic devices, are no longer sufficient to enhance the cybersecurity of existing systems. In some cases, it may even be impossible to fix security vulnerabilities in a system, indicating that cybersecurity was not adequately considered during the system's initial design.

Addressing this issue, the concept of security by design has been highlighted in the literature as a solution. This approach emphasizes incorporating security measures from the very beginning of the system design process rather than attempting to patch vulnerabilities as an afterthought. By adopting security by design principles, military organizations can proactively integrate robust security measures into their IoT deployments, mitigating risks and protecting sensitive military information. In summary, the security implications cannot be ignored as IoT technologies find their way into military applications. The increased attack surfaces, combined with hackers' targeting of the military domain, necessitate a shift towards a proactive approach to cybersecurity. Implementing security by design principles and adopting advanced security measures will be essential for safeguarding military systems and achieving military objectives in an increasingly connected and vulnerable world.

3.5 IoT Security and Education

In recent years, the IoT has profoundly impacted educational institutions, revolutionizing communication by enabling Internet-based connectivity between physical objects, sensors, and controllers. This transformative platform allows for measuring and analyzing various parameters within the educational environment through integrating sensors, big data, wearable technologies,

and cloud computing. While security has always been a critical consideration in the field of education, the advent of IoT technology introduces new security challenges. As communication and complexity increase within IoT-enabled educational systems, so do security concerns. The interconnected nature of IoT devices and the data they generate make educational institutions vulnerable to cyberattacks.

Protecting the security of educational IoT systems is of utmost importance. Breaches in security can result in the compromise of sensitive student and faculty data, disruption of critical educational services, and potential privacy violations. It is crucial for educational institutions to proactively address these security concerns and implement robust security measures. Security solutions for educational IoT environments should include authentication mechanisms to ensure that only authorized individuals and devices can access and interact with the system. Encryption protocols should be employed to secure data transmission and storage, safeguarding sensitive information from unauthorized access. Regular monitoring and vulnerability assessments should be conducted to identify and address potential weaknesses in the system. Additionally, educating students, faculty, and staff about cybersecurity best practices can help create a culture of awareness and responsible usage of IoT devices within educational settings. By prioritizing IoT security in education, institutions can leverage the benefits of IoT technology while mitigating the risks associated with cyber threats. A comprehensive approach to security will protect the integrity and confidentiality of educational data and ensure a safe and secure learning environment for students and educators alike.

3.6 IoT Security and Industry

The Industrial IoT (IIoT) is a paradigm shift, primarily in the domain of the manufacturing industry. In addition to improved operational efficiency in the production process, embedded technologies provide smart object identification mechanisms, intelligent automation capabilities, and around-the-clock monitoring capabilities, making the concept highly attractive to most industrial sectors. Moreover, it reduces worker intervention in hazardous industrial environments. The IIoT can be used in factories, materials handling, assembly lines, production processes, finalizing goods, and inbound and outbound logistics. Currently, IoT technologies are the basis for the growth of the IIoT phenomenon in many spheres, industrial, commercial, and social.

3.7 IoT Security and Smart Cities

With emerging network technologies such as fog computing and IoT, smart cities can be built more efficiently, fostering urban business, industry, tourism, and transportation management. Therefore, the development of a smart city will greatly boost its vast development potential. Due to the widespread implementation of smart systems, privacy, and security issues have become major challenges that require effective countermeasures. However, smart cities' heterogeneity, scalability, and dynamic characteristics make it impossible to apply traditional cybersecurity protection strategies directly. The design and implementation of new mechanisms and systems must be conscious of security and privacy risks.

3.8 IoT Security and Smart Grid

The IoT plays an important role in smart grids by monitoring and managing different parameters of power systems using the Internet. It automates the work for easy organization. Additionally, it allows the collection, analysis, and monitoring of a large amount of data from various sources, such as social media, machines, etc. As smart appliances, such as smartphones and smart watches, are becoming more common, IoT technology is becoming more prevalent in wireless technology. IoT-connected devices continue to grow at a rapid pace, posing many challenges in terms of security. Smart grids based on IoT would potentially contain millions of nodes, making them the most vulnerable to IoT-based cyberattacks.

3.9 IoT Security and Agriculture

Farmers can lower farming costs, improve irrigation efficiency, and enhance crop yields by leveraging IoT technology. This is a technologically advanced agricultural approach that combines agriculture and cutting-edge technologies. As IoT-based agriculture becomes more widely used, it may become more vulnerable to adversaries, posing new security and privacy risks and requiring enhanced communication security.

3.10 IoT Security and Smart Home

The smart home is a networked environment consisting of heterogeneous electronic devices and appliances that provide smart services to individuals on a ubiquitous basis. Application security levels determine the adoption rate of IoT devices in the smart home. In a smart home, IoT-enabled

applications must be designed with robust security mechanisms to ensure their users' privacy. IoT solutions include multiple elements: embedded devices, user interfaces, cloud computing for data processing, device control, etc. Implementing security and privacy features presents a functionality challenge.

3.11 IoT Security and Supply Chain

The rapidly evolving IoT ecosystem poses a growing threat to the supply chain. Various industries use IoT to secure their supply chains by tracking assets, raw materials, and supplies. Nevertheless, the security of the IoT supply chain is not generally addressed. In contrast to traditional systems, the IoT does not come from a single manufacturer or supplier. Rather, it consists of many interconnected components manufactured, designed, and operated by different entities around the world.

3.12 IoT Security and Banking System

Nowadays, banking and other financial systems face various security concerns around the globe. Security systems in banks are monitored and controlled only by banking authorities. Regarding banks, each locker owner lacks knowledge of what is happening with his/her valuable assets or lockers. Banks rarely compensate for lost items in safe deposit boxes when valuables are stolen or burglarized.

4 IoT Privacy and Security Solutions

4.1 LoRaWAN Security

The LOWPAN network, also known as 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network), is a wireless network protocol specifically designed for low-power devices with limited processing capabilities. It aims to enable communication between such devices and the Internet by leveraging IPv6 addressing and routing mechanisms. Despite being well designed, many researchers have raised security concerns about the LoRaWAN network. Despite having basic security properties, it is vulnerable to the following threats. Its join procedure is vulnerable, which is exploitable by replay attacks. The protocol also lacks end-to-end security because the application session key is established via the core network. The LoRaWAN network server can easily track the traffic between the two parties. The third issue is

that network and application session keys cannot guarantee perfect forward secrecy since they are based on long-term shared keys. The long-term key of a device can also be exposed when it is broken or compromised. This allows past session keys and encrypted data to be retrieved. A successful LoRaWAN network settlement is clearly hampered by the security flaws described above. To protect LOWPAN networks, only approved users should be able to access records, data integrity must be maintained, and malicious intruders must be prevented. An intrusion detection system is required to track traffic on both sides. LOWPAN's packet fragmentation framework is vulnerable due to its lack of encryption at the 6LoWPAN layer, optimal semiannual effort on fracture connections, and limited system memory.

4.2 Security in RPL

The IPv6 Routing Protocol for LLN (RPL) is designed to route IPv6 traffic in low-power networks over 6LoRaWPANs that experience high or inconsistent packet loss. In low-power networks deployed over 6LoWPANs with high or inconsistent packet loss mounts [102]. To protect RPL messages, a security field is added to the ICMPv6 message header. The information provided in this area indicates the security level and encryption algorithm used to encrypt messages. Data authentication, semantic security, replay protection, and key management are all supported by Low Data Rate (LDR). The RPL attacks include selective transmission, sinkhole, Sybil, hello-inundations, hyperspace, black hole, and denial of service.

4.3 Identity Tracking

The term identity tracking refers to the capability of a malicious entity to associate a device's address with a specific user's identity and physically track that user. A regular change of private addresses can tackle this thread.

4.4 Zigbee Security

Authentication is one of the key challenges in Zigbee security. In the case of the addition of a device to the network, distinguishing it from malicious devices is challenging. With Zigbee 3.0, this problem is solved by introducing a new join mechanism called installation code. A Zigbee installation code, known as an install code, consists of 18 bytes. The code is also stored inside the device. Smartphone applications can be used to scan the code and send it to the coordinator. Through the AES-MMO algorithm, a link key is derived

from the installation code as a pre-configured secret. The coordinator uses the link key during the join procedure to encrypt the initial transport key message. Decrypting the transport key message and joining the network is only possible for devices with the code.

4.5 RFID Security

Authentication and privacy are fundamental concerns in RFID security. RFID tags and readers can be authenticated through a secure protocol. The tagged product is considered authentic if the RFID reader and the RFID tag convince the RFID reader that both possess secret information. The untraceability of tags is one of the most important properties of tag anonymity, as it ensures the privacy of RFID tags or the mobility of their users. One of the efficient ways to accomplish this attribute is to encode the original identity of the tag using a cryptographic primitive, for example, a one-way collision-resistant hash function.

4.6 Ensure Device Authentication

Authentication is another method to strengthen the security level of IoT devices, preventing unauthorized access to data. In this regard, an attacker must obtain certain information in order to compromise a device. Therefore, this method of user authentication is a better option for IoT devices.

4.7 Secure the Network

Endpoint security serves as the first line of defense for each system connected to the IoT network. Anti-malware and antivirus software are crucial components of endpoint security, protecting various forms of malicious software, including viruses, worms, and trojans. These tools continuously monitor the system for any signs of malware and actively work to detect, quarantine, and eliminate threats, preventing potential damage or unauthorized access. In addition to anti-malware and antivirus solutions, intrusion prevention systems (IPS) play a vital role in safeguarding the system. IPS monitors network traffic in real-time, analyzing and identifying suspicious or malicious activities. By using predefined rules and heuristics, IPS can block or mitigate threats, such as unauthorized access attempts, network-based attacks, or abnormal behavior patterns. This proactive defense mechanism adds an extra layer of security to the system, reducing the risk of successful cyberattacks.

4.8 Use Public Key Infrastructure

Public key infrastructure is the most trustworthy method used by many companies. Using this process, digital data can be created, managed, and distributed on IoT devices. The PKI ensures data protection from both ends, i.e., from the user and from the sender, as the data is encrypted and then decrypted at the user's end. To prevent the changing of data and cyberattacks, secret keys are used to transfer or communicate.

4.9 Use IoT Security Analytics

In order to detect security flaws in IoT devices through analytics, we can apply security analytics. Analytics is useful for identifying loopholes in applications or IoT devices. IoT security can be provided through the collection of data from multiple sources. Performing security analytics monitoring on IoT devices from the IoT gateway alone can also reduce malicious and normal behaviors in IoT devices. This will assist security experts in recognizing this anomaly in the data that could harm IoT devices.

5 IoT Privacy and Security Challenges

As more IoT-related actions are carried out, a growing number of security holes will emerge. As more devices and services become connected to the internet, the opportunities for malicious actors to exploit these connections increase. This can lead to the theft of personal information, the hijacking of connected devices, and other security threats. Extended risk can result in restrictions and missed opportunities for improving security. In order to achieve IoT security, the following challenges must be addressed.

- User privacy: Actions must be taken to secure client information (both for outside and internal clients). IoT devices provided by managers are utilized by many professionals. An organization's reputation will suffer when private information is compromised, which is why this is one of the best IoT security challenges that should not be overlooked. Passwords set by default on several IoT devices are weak. Although it is recommended that passwords be modified, few IT managers adhere to this basic recommendation.
- Infrequent updates: IT experts use programming updates to make sure that PCs and cell phones are as secure as possible. Some IoT devices may not receive the same amount of programming updates as other advances. This is because the programming updates require specific

knowledge of the device and its architecture, which may not be available to the experts. Additionally, these updates may not be released as frequently as other devices due to the potentially limited market size of the device.

- Inability to predict threats: The security community must be proactive in order to prevent IoT security breaches before they occur. Nonetheless, a couple of attempts may not be sufficient to establish a solid organizational structure that would screen activities and provide information about potential threats. To ensure proper security protocols, organizations need to employ a multi-layered approach, which includes education and awareness training for employees, as well as risk assessments, vulnerability scans, and regular monitoring of systems and networks. Additionally, organizations should develop processes to respond to any potential security incidents in a timely manner.
- Phishing attacks: Phishing has become a major security issue across all organizational advancements, and IoT devices are the latest vector for attack. Although phishing is one of the most widely perceived forms of security threat, many organizations fail to adequately train their employees regarding the latest phishing threats, regardless of the fact that this is one of the most widely recognized forms of security threat.
- Botnets aimed at cryptocurrency: There is heated mining competition, and hackers are using this as a chance to cash in on the crypto craze, while some blockchain resists hacking, the main problem does not lie in blockchain but not app development, which is running on itself. There is a method called social engineering, which is used to extract credentials. Open-source money is digital currency aside from many others, which are mined with IoT devices; so many hackers have diverted the IP and video cameras to mine crypto.
- Malware and ransomware: Since the number of IoT-connected devices is increasing, malware and ransomware are being used to exploit them. Ransomware uses encryption in order to lock users out of their devices. There is a fusion between malware and ransomware that creates a completely new type of attack and its hybridization. Ransomware attacks can interfere with traffic flow, disable devices, or steal data from users.

6 Conclusion

Currently, the technological age has had a wide-ranging impact on all behaviors and lives, and this impact has drawn the attention of the general public

and companies to this issue. For more than a decade, the concept of IoT has been formed. Information technology business has created a new vision encompassing all technological, social, and economic ideas. Integrating technology and communication strategy are essential factors in the widespread use of IoT. With the fast expansion of IoT, these networks generate large amounts of data every day, making data the most important source of information today. Ensuring the security and privacy of IoT services and applications is a significant factor in building trust in users and using the IoT platform. Considering the above, this paper presented a thorough overview of different security and privacy solutions, along with outlining key challenges.

References

[1] B. Pourghebleh, N. Hekmati, Z. Davoudnia, and M. Sadeghi, "A roadmap towards energy-efficient data fusion methods in the Internet of Things," Concurrency and Computation: Practice and Experience, p. e6959, 2022.

[2] B. Pourghebleh, A. A. Anvigh, A. R. Ramtin, and B. Mohammadi, "The importance of nature-inspired meta-heuristic algorithms for solving virtual machine consolidation problem in cloud environments," Cluster Computing, pp. 1–24, 2021.

[3] C. Han and X. Fu, "Challenge and Opportunity: Deep Learning-Based Stock Price Prediction by Using Bi-Directional LSTM Model," Frontiers in Business, Economics and Management, vol. 8, no. 2, pp. 51–54, 2023.

[4] M. Shahin et al., "Cluster-based association rule mining for an intersection accident dataset," in 2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), 2021: IEEE, pp. 1–6.

[5] B. M. Jafari, M. Zhao, and A. Jafari, "Rumi: An Intelligent Agent Enhancing Learning Management Systems Using Machine Learning Techniques," Journal of Software Engineering and Applications, vol. 15, no. 9, pp. 325–343, 2022.

[6] S. Yumusak, S. Layazali, K. Oztoprak, and R. Hassanpour, "Low-diameter topic-based pub/sub overlay network construction with minimum–maximum node degree," PeerJ Computer Science, vol. 7, p. e538, 2021.

[7] R. N. Jacob, "Non-performing Asset Analysis Using Machine Learning," in ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1, 2021: Springer, pp. 11–18.

[8] S. Meisami, M. Beheshti-Atashgah, and M. R. Aref, "Using Blockchain to Achieve Decentralized Privacy In IoT Healthcare," arXiv preprint arXiv:2109.14812, 2021.

[9] H. Seraji, R. Tavakkoli-Moghaddam, S. Asian, and H. Kaur, "An integrative location-allocation model for humanitarian logistics with distributive injustice and dissatisfaction under uncertainty," Annals of Operations Research, vol. 319, no. 1, pp. 211–257, 2022.

[10] M. Sadi et al., "Special Session: On the Reliability of Conventional and Quantum Neural Network Hardware," in 2022 IEEE 40th VLSI Test Symposium (VTS), 2022: IEEE, pp. 1–12.

[11] M. Sarbaz, M. Manthouri, and I. Zamani, "Rough neural network and adaptive feedback linearization control based on Lyapunov function," in 2021 7th International Conference on Control, Instrumentation and Automation (ICCIA), 2021: IEEE, pp. 1–5.

[12] H. Kosarirad, M. Ghasempour Nejati, A. Saffari, M. Khishe, and M. Mohammadi, "Feature Selection and Training Multilayer Perceptron Neural Networks Using Grasshopper Optimization Algorithm for Design Optimal Classifier of Big Data Sonar," Journal of Sensors, vol. 2022, 2022.

[13] S. Ahmad, S. Umirzakova, F. Jamil, and T. K. Whangbo, "Internet-of-things-enabled serious games: A comprehensive survey," Future Generation Computer Systems, 2022.

[14] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9326–9337, 2019.

[15] K. Cao et al., "Enhancing physical layer security for IoT with non-orthogonal multiple access assisted semi-grant-free transmission," IEEE Internet of Things Journal, 2022.

[16] V. Hayyolalam, B. Pourghebleh, and A. A. Pourhaji Kazem, "Trust management of services (TMoS): Investigating the current mechanisms," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 10, p. e4063, 2020.

[17] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research," Journal of Network and Computer Applications, vol. 97, pp. 23–34, 2017.

[18] B. Pourghebleh and V. Hayyolalam, "A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things," Cluster Computing, pp. 1–21, 2019.
[19] B. Pourghebleh, V. Hayyolalam, and A. A. Anvigh, "Service discovery in the Internet of Things: review of current trends and research challenges," Wireless Networks, vol. 26, no. 7, pp. 5371–5391, 2020.
[20] S. Ammirato, F. Sofo, A. M. Felicetti, and C. Raso, "A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context," European Journal of Innovation Management, 2018.
[21] E. S. M. Nordin, H. Abas, and A. Azizan, "Modelling IoT Security Risk Management in Banking Environment," Open International Journal of Informatics, vol. 8, no. 1, pp. 10–20, 2020.
[22] R. E. Hiromoto, M. Haney, and A. Vakanski, "A secure architecture for IoT with supply chain risk management," in 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017, vol. 1: IEEE, pp. 431–435.
[23] T. Omitola and G. Wills, "Towards mapping the security challenges of the Internet of Things (IoT) supply chain," Procedia Computer Science, vol. 126, pp. 441–450, 2018.
[24] W. Zhou and S. Piramuthu, "IoT security perspective of a flexible healthcare supply chain," Information Technology and Management, vol. 19, no. 3, pp. 141–153, 2018.
[25] L. Nandakumar, "Privacy-Aware State Estimation based on Obfuscated Transformation and Differential Privacy: With applications to smart grids and supply chain economics," 2018.
[26] M. J. Farooq and Q. Zhu, "IoT supply chain security: overview, challenges, and the road ahead," arXiv preprint arXiv:1908.07828, 2019.
[27] A. Shahzad, K. Zhang, and A. Gherbi, "Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive blockchain," Sensors, vol. 20, no. 13, p. 3760, 2020.
[28] D. Guo, "Internet of Things Based Network Security for Supply Chain Management in the Business Environment," Wireless Personal Communications, pp. 1–22, 2021.
[29] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home

IoT devices," in 2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob), 2015: IEEE, pp. 163–167.

[30] F. K. Santoso and N. C. Vun, "Securing IoT for smart home system," in 2015 international symposium on consumer electronics (ISCE), 2015: IEEE, pp. 1–2.

[31] P. Gupta and J. Chhabra, "IoT based Smart Home design using power and security management," in 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016: IEEE, pp. 6–10.

[32] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," Information, vol. 7, no. 3, p. 44, 2016.

[33] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 2017: IEEE, pp. 618–623.

[34] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," in 2017 23rd International Conference on Automation and Computing (ICAC), 2017: IEEE, pp. 1–6.

[35] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017: IEEE, pp. 1292–1297.

[36] S. Marksteiner, V. J. E. Jiménez, H. Valiant, and H. Zeiner, "An overview of wireless IoT protocol security in the smart home domain," 2017 Internet of Things Business Models, Users, and Networks, pp. 1–8, 2017.

[37] D. Bastos, M. Shackleton, and F. El-Moussa, "Internet of things: A survey of technologies and security risks in smart home and city environments," 2018.

[38] Z. Shouran, A. Ashari, and T. Priyambodo, "Internet of things (IoT) of smart home: privacy and security," International Journal of Computer Applications, vol. 182, no. 39, pp. 3–8, 2019.

[39] T. Baranwal and P. K. Pateriya, "Development of IoT based smart security and monitoring devices for agriculture," in 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence), 2016: IEEE, pp. 597–602.

[40] B. Keerthana, P. Nivetha, M. Boomika, M. Mathivathani, and A. Niranjana, "IoT based smart security and monitoring devices for agriculture," Int. J. Inf. Res. Rev, vol. 5, no. 04, pp. 5415–5419, 2018.
[41] L. S. Shabadi and H. B. Biradar, "Design and implementation of IOT based smart security and monitoring for connected smart farming," International Journal of Computer Applications, vol. 975, no. 8887, 2018.
[42] V. Nithin, S. Mishra, P. Devarubiny, and S. Muthulakshmi, "IoT enabled farming assist and security using machine learning," ed: Asian Research Publishing Network Journal of Engineering and Applied Sciences, 2019.
[43] T. Gundu and V. Maronga, "IoT Security and Privacy: Turning on the Human Firewall in Smart Farming," ICICIS, pp. 95–104, 2019.
[44] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural IoT and smart farming," Sensors, vol. 20, no. 22, p. 6458, 2020.
[45] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," IEEE access, vol. 8, pp. 32031–32053, 2020.
[46] A. Vangala, A. K. Das, N. Kumar, and M. Alazab, "Smart secure sensing for IoT-based agriculture: Blockchain perspective," IEEE Sensors Journal, vol. 21, no. 16, pp. 17591–17607, 2020.
[47] H. N. Saha, R. Roy, M. Chakraborty, and C. Sarkar, "Development of IoT-based smart security and monitoring devices for agriculture," Agricultural informatics: automation using the IoT and machine learning, pp. 147–169, 2021.
[48] G. J. Rosline, P. Rani, and D. Gnana Rajesh, "Comprehensive Analysis on Security Threats Prevalent in IoT-Based Smart Farming Systems," in Ubiquitous Intelligent Systems: Springer, 2022, pp. 185–194.
[49] S. Sharma and P. Mittal, "IoT-Based Smart Security System for Agriculture Fields," in Cyber Security and Digital Forensics: Springer, 2022, pp. 143–151.
[50] M. Sherburne, R. Marchany, and J. Tront, "Implementing moving target ipv6 defense to secure 6lowpan in the internet of things and smart grid," in Proceedings of the 9th Annual Cyber and Information Security Research Conference, 2014, pp. 37–40.
[51] C. Bekara, "Security issues and challenges for the IoT-based smart grid," Procedia Computer Science, vol. 34, pp. 532–537, 2014.

[52] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," IEEE Communications Magazine, vol. 55, no. 10, pp. 70–75, 2017.
[53] Z. Guan, J. Li, L. Wu, Y. Zhang, J. Wu, and X. Du, "Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1934–1944, 2017.
[54] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36–49, 2019.
[55] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," Internet of things, vol. 14, p. 100111, 2021.
[56] R. Borgaonkar, I. Anne Tøndel, M. Zenebe Degefa, and M. Gilje Jaatun, "Improving smart grid security through 5G enabled IoT and edge computing," Concurrency and Computation: Practice and Experience, vol. 33, no. 18, p. e6466, 2021.
[57] A. Saleem et al., "FESDA: Fog-enabled secure data aggregation in smart grid IoT network," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6132–6142, 2019.
[58] J.-M. Bohli, A. Skarmeta, M. V. Moreno, D. García, and P. Langendörfer, "SMARTIE project: Secure IoT data management for smart cities," in 2015 International Conference on Recent Advances in Internet of Things (RIoT), 2015: IEEE, pp. 1–6.
[59] A. W. Burange and H. D. Misalkar, "Review of Internet of Things in development of smart cities with data management & privacy," in 2015 International Conference on Advances in Computer Engineering and Applications, 2015: IEEE, pp. 189–195.
[60] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 716–723, 2017.
[61] S. Latif and N. A. Zafar, "A survey of security and privacy issues in IoT for smart cities," in 2017 Fifth International Conference on Aerospace Science & Engineering (ICASE), 2017: IEEE, pp. 1–5.
[62] N. Magaia, R. Fonseca, K. Muhammad, A. H. F. N. Segundo, A. V. L. Neto, and V. H. C. de Albuquerque, "Industrial internet-of-things security enhanced with deep learning approaches for smart cities," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6393–6405, 2020.

[63] C. Toma, A. Alexandru, M. Popa, and A. Zamfiroiu, "IoT solution for smart cities' pollution monitoring and the security challenges," Sensors, vol. 19, no. 15, p. 3401, 2019.
[64] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7702–7712, 2019.
[65] F. Al-Turjman and J. P. Lemayian, "Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview," Computers & Electrical Engineering, vol. 87, p. 106776, 2020.
[66] S. Chakrabarty and D. W. Engels, "Secure smart cities framework using IoT and AI," in 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), 2020: IEEE, pp. 1–6.
[67] Z. Lv, L. Qiao, A. Kumar Singh, and Q. Wang, "AI-empowered IoT security for smart cities," ACM Transactions on Internet Technology, vol. 21, no. 4, pp. 1–21, 2021.
[68] D. Janeera, S. Gnanamalar, K. Ramya, and A. Kumar, "Internet of things and artificial intelligence-enabled secure autonomous vehicles for smart cities," in Automotive Embedded Systems: Springer, 2021, pp. 201–218.
[69] K.-Y. Lam, S. Mitra, F. Gondesen, and X. Yi, "ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities," IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5895–5908, 2021.
[70] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making use of semiconductor manufacturing process variations: FinFET-based physical unclonable functions for efficient security integration in the IoT," Analog integrated circuits and signal processing, vol. 93, no. 3, pp. 429–441, 2017.
[71] C. Toma and M. Popa, "IoT security approaches in oil & gas solution industry 4.0," Informatica Economica, vol. 22, no. 3, pp. 46–61, 2018.
[72] Z. Shahbazi and Y.-C. Byun, "Integration of Blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing," Sensors, vol. 21, no. 4, p. 1467, 2021.
[73] J. R. Reidenberg and F. Schaub, "Achieving big data privacy in education," Theory and Research in Education, vol. 16, no. 3, pp. 263–279, 2018.

[74] S. M. T. Toapanta, J. M. V. López, R. S. T. Soledispa, and L. E. M. Gallegos, "Definition of a security prototype for IoT applied to higher education," in 2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4), 2019: IEEE, pp. 115–120.

[75] A. Badshah, A. Ghani, M. A. Qureshi, and S. Shamshirband, "Smart security framework for educational institutions using internet of things (IoT)," Comput. Mater. Contin, vol. 61, no. 1, pp. 81–101, 2019.

[76] K. M. Jones et al., ""We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education," Journal of the Association for Information Science and Technology, vol. 71, no. 9, pp. 1044–1059, 2020.

[77] L. A. Alexei and A. Alexei, "Analysis of IoT security issues used in Higher Education Institutions," International Journal Of Mathematics And Computer Research, no. 5, pp. 2277–2286, 2021.

[78] M. A. Canbaz, K. OHearon, M. McKee, and M. N. Hossain, "IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond," in 2021 ASEE Virtual Annual Conference Content Access, 2021.

[79] J. S. Owlett, K. A. R. Richards, S. R. Wilson, J. DeFreese, and F. Roberts, "Privacy management in the military family during deployment: Adolescents' perspectives," Journal of family communication, vol. 15, no. 2, pp. 141–158, 2015.

[80] J. Chudzikiewicz, J. Furtak, and Z. Zielinski, "Secure protocol for wireless communication within internet of military things," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015: IEEE, pp. 508–513.

[81] K. Wrona, "Securing the Internet of Things a military perspective," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015: IEEE, pp. 502–507.

[82] J. Furtak, Z. Zieliñski, and J. Chudzikiewicz, "Security techniques for the WSN link layer within military IoT," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016: IEEE, pp. 233–238.

[83] Z. Zieliski, J. Chudzikiewicz, and J. Furtak, "An approach to integrating security and fault tolerance mechanisms into the military IoT," in Security and fault tolerance in Internet of Things: Springer, 2019, pp. 111–128.

[84] M. S. Arafath, K. U. R. Khan, and K. Sunitha, "Incorporating privacy and security in military application based on opportunistic sensor

network," International Journal of Internet Technology and Secured Transactions, vol. 7, no. 4, pp. 295–316, 2017.

[85] A. R. Sfar, Z. Chtourou, and Y. Challal, "A systemic and cognitive vision for IoT security: a case study of military live simulation and security challenges," in 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C), 2017: IEEE, pp. 101–105.

[86] S. Cha, S. Baek, S. Kang, and S. Kim, "Security evaluation framework for military IoT devices," Security and Communication Networks, vol. 2018, 2018.

[87] B. E. Katalin, "Possibilities and Security Challenges of Using IoT For Military Purposes," Hadmérnök, vol. 13, no. 3, pp. 378–390, 2018.

[88] M. Pradhan and J. Noll, "Security, privacy, and dependability evaluation in verification and validation life cycles for military IoT systems," IEEE Communications Magazine, vol. 58, no. 8, pp. 14–20, 2020.

[89] W. Labda, N. Mehandjiev, and P. Sampaio, "Modeling of privacy-aware business processes in BPMN to protect personal data," in Proceedings of the 29th Annual ACM Symposium on Applied Computing, 2014, pp. 1399–1405.

[90] V. Kharchenko, M. Kolisnyk, I. Piskachova, and N. Bardis, "Reliability and security issues for IoT-based smart business center: architecture and Markov model," in 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 2016: IEEE, pp. 313–318.

[91] V. Diamantopoulou, N. Argyropoulos, C. Kalloniatis, and S. Gritzalis, "Supporting the design of privacy-aware business processes via privacy process patterns," in 2017 11th International Conference on Research Challenges in Information Science (RCIS), 2017: IEEE, pp. 187–198.

[92] K. G. Chandrashekhar, F. Karimi-Alaghehband, and D. Özgün, "IoT Security Adoption into Business Processes: A Socio-Technical View," 2017.

[93] A. Bujari, M. Furini, F. Mandreoli, R. Martoglia, M. Montangero, and D. Ronzani, "Standards, security and business models: key challenges for the IoT scenario," Mobile Networks and Applications, vol. 23, no. 1, pp. 147–154, 2018.

[94] H. E. Yılmaz, A. Sirel, and M. F. Esen, "The impact of internet of things self-security on daily business and business continuity," in Research Anthology on Business Continuity and Navigating Times of Crisis: IGI Global, 2022, pp. 695–712.

[95] J. Pacheco, S. Satam, S. Hariri, C. Grijalva, and H. Berkenbrock, "IoT Security Development Framework for building trustworthy Smart car services," in 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 2016: IEEE, pp. 237–242.

[96] S. Wang, Y. Hou, F. Gao, and X. Ji, "A novel IoT access architecture for vehicle monitoring system," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016: IEEE, pp. 639–642.

[97] D. Mukhopadhyay, M. Gupta, T. Attar, P. Chavan, and V. Patel, "An attempt to develop an IOT based vehicle security system," in 2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS), 2018: IEEE, pp. 195–198.

[98] B. Girish, A. D. Gowda, H. Amreen, and K. A. Singh, "IOT based security system for smart vehicle," International Research Journal of Engineering and Technology (IRJET), vol. 5, no. 5, pp. 2869–2874, 2018.

[99] I. García-Magariño, S. Sendra, R. Lacuesta, and J. Lloret, "Security in vehicles with IoT by prioritization rules, vehicle certificates, and trust management," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 5927–5934, 2018.

[100] A. R. Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in IoT-based transportation," IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 12, pp. 4405–4414, 2019.

[101] M. M. Hussain, M. S. Alam, M. S. Beg, and R. Ali, "Searching for IoT Resources in Intelligent Transportation Cyberspace (T-CPS)—Requirements, Use-Cases and Security Aspects," in Cybersecurity and Privacy in Cyber-Physical Systems: CRC Press, 2019, pp. 293–331.

[102] A. Lei, Y. Cao, S. Bao, P. Asuquom, H. Cruickshank, and Z. Sun, "Blockchain-based dynamic key management for IoT-transportation security protection," Blockchain for Distributed Systems Security, p. 117, 2019.

[103] N. Vinayaga-Sureshkanth, R. Wijewickrama, A. Maiti, and M. Jadliwala, "Security and privacy challenges in upcoming intelligent urban micromobility transportation systems," in Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security, 2020, pp. 31–35.

[104] J. Zhang, Y. Wang, S. Li, and S. Shi, "An architecture for IoT-enabled smart transportation security system: a geospatial approach," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6205–6213, 2020.

[105] W. Priharti, S. Sumaryo, T. Saraswati, and M. Nurfadilah, "IoT based logistics vehicle security monitoring system," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 771, no. 1: IOP Publishing, p. 012012.
[106] M. Hammoudeh et al., "A service-oriented approach for sensing in the Internet of Things: intelligent transportation systems and privacy use cases," IEEE Sensors Journal, vol. 21, no. 14, pp. 15753–15761, 2020.
[107] K. Abbas et al., "Convergence of blockchain and IoT for secure transportation systems in smart cities," Security and Communication Networks, vol. 2021, 2021.
[108] A. Masood and A. Gupta, "Enhanced Logistics Security Techniques Using IoT and 5G," in 2020 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 2020: IEEE, pp. 7–14.
[109] I. Sergi, T. Montanaro, F. L. Benvenuto, and L. Patrono, "A smart and secure logistics system based on IoT and cloud technologies," Sensors, vol. 21, no. 6, p. 2231, 2021.
[110] Y. Abbassi and H. Benlahmer, "IoT and Blockchain combined: for decentralized security," Procedia Computer Science, vol. 191, pp. 337–342, 2021.
[111] A. J. J. Valera, M. A. Zamora, and A. F. Skarmeta, "An architecture based on internet of things to support mobility and security in medical environments," in 2010 7th IEEE consumer communications and networking conference, 2010: IEEE, pp. 1–5.
[112] L. M. R. Tarouco et al., "Internet of Things in healthcare: Interoperatibility and security issues," in 2012 IEEE international conference on communications (ICC), 2012: IEEE, pp. 6121–6125.
[113] A. Rghioui, A. L'aarje, F. Elouaai, and M. Bouhorma, "The internet of things for healthcare monitoring: security review and proposed solution," in 2014 Third IEEE international colloquium in information science and technology (CIST), 2014: IEEE, pp. 384–389.
[114] J. T. Kim, "Privacy and security issues for healthcare system with embedded rfid system on internet of things," Advanced Science and Technology Letters, vol. 72, pp. 109–112, 2014.
[115] S.-h. Woo, "Medical Information Security and Standard Technology On IoT Environment," Journal of the Korea Institute of Information and Communication Engineering, vol. 19, no. 11, pp. 2683–2688, 2015.
[116] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in 2015 Seventh

International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), 2015: IEEE, pp. 217–222.

[117] E. Al Alkeem, C. Y. Yeun, and M. J. Zemerly, "Security and privacy framework for ubiquitous healthcare IoT devices," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015: IEEE, pp. 70–75.

[118] U. Computing, "Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)," in 2015 IEEE International Conference on. IEEE, 2015.

[119] P. A. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 2016: IEEE, pp. 30–35.

[120] K.-H. Han and W.-S. Bae, "Proposing and verifying a security-enhanced protocol for IoT-based communication for medical devices," Cluster Computing, vol. 19, no. 4, pp. 2335–2341, 2016.

[121] N. S. Abouzakhar, A. Jones, and O. Angelopoulou, "Internet of things security: A review of risks and threats to healthcare sector," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017: IEEE, pp. 373–378.

[122] P. A. Wortman, F. Tehranipoor, N. Karimian, and J. A. Chandy, "Proposing a modeling framework for minimizing security vulnerabilities in IoT systems in the healthcare domain," in 2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), 2017: IEEE, pp. 185–188.

[123] D. Minoli, K. Sohraby, and B. Occhiogrosso, "Iot security (IoTsec) mechanisms for e-health and ambient assisted living applications," in 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2017: IEEE, pp. 13–18.

[124] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," Sensors, vol. 17, no. 7, p. 1482, 2017.

[125] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber security challenges of deploying IoT in smart cities for healthcare applications," in 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), 2018: IEEE, pp. 140–145.

[126] Y. Winnie, E. Umamaheswari, and D. Ajay, "Enhancing data security in IoT healthcare services using fog computing," in 2018 International Conference on Recent Trends in Advance Computing (ICRTAC), 2018: IEEE, pp. 200–205.
[127] V. Alagar, A. Alsaig, O. Ormandjiva, and K. Wan, "Context-based security and privacy for healthcare IoT," in 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), 2018: IEEE, pp. 122–128.
[128] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," IEEE Transactions on Industrial Informatics, vol. 14, no. 4, pp. 1656–1665, 2018.
[129] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical internet of things: a review," Security and Communication Networks, vol. 2018, 2018.
[130] T. Hayakawa, R. Sasaki, H. Hayashi, Y. Takahashi, T. Kaneko, and T. Okubo, "Proposal and application of security/safety evaluation method for medical device system that includes IoT," in Proceedings of the 2018 VII International Conference on Network, Communication and Computing, 2018, pp. 157–164.
[131] J. B. Martinez, "Medical device security in the IoT age," in 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2018: IEEE, pp. 128–134.
[132] A. Yeole, D. Kalbande, and A. Sharma, "Security of 6LoWPAN IoT networks in hospitals for medical data exchange," Procedia Computer Science, vol. 152, pp. 212–221, 2019.
[133] C. Bradley, S. El-Tawab, and M. H. Heydari, "Security analysis of an IoT system used for indoor localization in healthcare facilities," in 2018 Systems and Information Engineering Design Symposium (SIEDS), 2018: IEEE, pp. 147–152.
[134] S. Pirbhulal, N. Pombo, V. Felizardo, N. Garcia, A. H. Sodhro, and S. C. Mukhopadhyay, "Towards machine learning enabled security framework for IoT-based healthcare," in 2019 13th International Conference on Sensing Technology (ICST), 2019: IEEE, pp. 1–6.
[135] G. Srivastava, J. Crichigno, and S. Dhar, "A light and secure healthcare blockchain for iot medical devices," in 2019 IEEE Canadian conference of electrical and computer engineering (CCECE), 2019: IEEE, pp. 1–5.

[136] E. Fazeldehkordi, O. Owe, and J. Noll, "Security and privacy in IoT systems: a case study of healthcare products," in 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), 2019: IEEE, pp. 1–8.

[137] X. C. Yin, Z. G. Liu, B. Ndibanje, L. Nkenyereye, and S. Riazul Islam, "An IoT-based anonymous function for security and privacy in healthcare sensor networks," Sensors, vol. 19, no. 14, p. 3146, 2019.

[138] F. I. Salih, N. A. A. Bakar, N. H. Hassan, F. Yahya, N. Kama, and J. Shah, "IOT security risk management model for healthcare industry," Malaysian Journal of Computer Science, pp. 131–144, 2019.

[139] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in 2019 15th international conference on distributed computing in sensor systems (DCOSS), 2019: IEEE, pp. 457–464.

[140] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT," IEEE Access, vol. 7, pp. 135632–135649, 2019.

[141] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare internet of things," Wireless Networks, vol. 27, no. 8, pp. 5503–5509, 2021.

[142] A. Rahman, M. S. Hossain, N. A. Alrajeh, and F. Alsolami, "Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9603–9610, 2020.

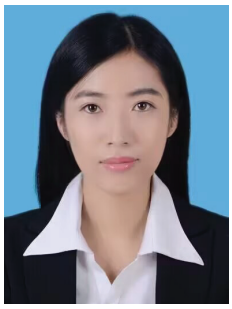
[143] M. Wazid, B. Bera, A. Mitra, A. K. Das, and R. Ali, "Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services," in Proceedings of the 2nd ACM MobiCom workshop on drone assisted wireless communications for 5G and beyond, 2020, pp. 37–42.

[144] M. Amoon, T. Altameem, and A. Altameem, "Internet of things sensor assisted security and quality analysis for health care data sets using artificial intelligent based heuristic health management system," Measurement, vol. 161, p. 107861, 2020.

[145] K. Nomikos, A. Papadimitriou, G. Stergiopoulos, D. Koutras, M. Psarakis, and P. Kotzanikolaou, "On a security-oriented design framework for medical IoT devices: The hardware security perspective," in 2020 23rd Euromicro Conference on Digital System Design (DSD), 2020: IEEE, pp. 301–308.

[146] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical IoT networks," Computer Communications, vol. 166, pp. 154–164, 2021.
[147] T. M. Ghazal, "Internet of things with artificial intelligence for health care security," Arabian Journal for Science and Engineering, 2021.
[148] S. Oniani, G. Marques, S. Barnovi, I. M. Pires, and A. K. Bhoi, "Artificial intelligence for internet of things and enhanced medical systems," in Bio-inspired neurocomputing: Springer, 2021, pp. 43–59.

Biography



Yujing Lu graduated from Hebei Normal University with a master's degree in software engineering in 2016. Presided over three department level projects, one municipal education reform project and one school level project, one of which won the third prize of Hebei human resources and social security research project. Published two papers. Her research interests include artificial intelligence, network security and intrusion detection.