Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

A Comprehensive Analysis on Privacy and Security for IoT Solutions

Muhammad Sharjeel[1*], Irshad Ahmed Sumra[2], Abdul Sattar[2], and Mahnoor Arshad[1]

[1]Department of Data Science, Lahore Garrison University, Lahore, Pakistan.
[2]Department of Computer Science, Lahore Garrison University, Lahore, Pakistan.
[*]Corresponding Author: Muhammad Sharjeel. Email: sharjeelafzal50@gmail.com

Received: March 11, 2024 **Accepted:** December 01, 2024

Abstract: The rapid growth of Internet of Things (IoT) applications has led to concerns regarding security and privacy due to the vast amounts of data collected by IoT devices and transmitted online. As a result, it is essential to explore strategies that can enhance the resilience of IoT systems against security vulnerabilities and privacy issues. In this paper, we first identify and discuss effective practices for ensuring IoT privacy and security, which consist of a series of procedures that can serve as guidelines for addressing privacy and security challenges in IoT systems. Furthermore, these best practices are applied to two practical use cases: a crowd monitoring system and a vehicle mobility system. This work provides a foundational reference for researchers and practitioners seeking to fortify IoT systems against evolving security and privacy risks.

Keywords: Internet of Things; IoT Security; Best practices; Non-Personal Data; Privacy by Design; Risk assessment.

1. Introduction

Telecommunications technologies and services have also emerged rapidly over the last decades leading to the demand for new legislation with regards to the processing of personal and non-personal information. to the requirement for a new regulation on the processing of personal and non-personal data. Nowadays, the Internet of Things (IoT) technology enables associating diverse objects such as traffic lights, cars, watches, surveillance cameras and so on. exchange information through Internet with each other. It appears clear that with increase in the number of innovations in the telecommunications services, the higher the amount of data. producers and data consumers [1]. Accordingly, there is a rise in the categories of data being shared, which include non-personal as well personal information. Moreover, with the IoT revolution, the subjects to be used in the data communication have suggested that people as well as things and tool in manufacturing process. Paloalto in their report of 2020 established that 98 percent of organizations encounter at least one cyber-attack in their lifetime. it reveals personal details since the overall IoT traffic, is unencrypted. and delicate information in the Internet [2]. Furthermore, as found in the previous iteration, more than half of IoT devices globally are open to attacks ranked from medium to high. Therefore, there is the need to determine how data exchange of Internet of things applications have to be handled in order to minimize on the users' privacy and security risks.

A productive interaction takes place between things, objects and persons thus enabling the datafication process that turns people's actions into data. Furthermore, as there is tight concord between products and people, activities and interactions of Activities which are associated to individuals (for instance sleeping, working or playing sports) can be datified. This can be achieved for instance through purchase, tracking or the process of obtaining more information of the company. and corridor planning including the positioning of people and their movements across. smartphones, smart watches, social network sites along with many other smart devices. devices [3]. In this regard, we think that it is necessary to make a clear differentiation between personal data and non-personal data the distinction can be predicted from the data producer. In fact, the how of data production proves to be a pragmatic method to identify the private. or the type, meaning, or scope of the received or collected information – personal or non-personal. In the IoT world, sources of data can be the user and the connected object. In the IoT world, data provider is configurable as a user and the connected object. In the first case, the data are absolutely personal data that refer to the owner of the object. In the second case, data generated by the object can be PDR if data concerning the owner of the object are collected, or non-PDR, for example, basic technical data (how much oil is left in the car's tank or how much electricity a household appliance has used is collected) or non-personal data, such as simple technical data (the level of oil in the engine of a vehicle or the power consumed by a household appliance) [4].

The advancement of industrial technology in telecommunications, in concerning the capillarity of the network, type and quantity. of carrying data that is to be transmitted and stored in to focus has made to enable even an evolution from a legal and regulatory perspective of view. However, identifying and localizing IoT or introducing with it an identifiable seriality raises problems. concerning the processing of personal data and protection of data subjects to which the information relates. From the access to/touch points of frequently used items or devices such as typical mobile device, slate, personal car, when, for instance, large number of smoothly interconnected IoT objects in smart house environment is also here possible to track individual, their location, daily routine, and actions. Nowadays, security is observed in situations like roads, cars and other things. houses, and also the continuous increasing in production and consumption of new consumer goods and Sumption of products. IoT security is the process by which the systems of IoT are protected from vulnerabilities that may work against their functioning. safe [5], which means to shield the IoT system from IoT security. challenges include; challenges to authentication, confidentiality, integrity and availability. availability [6-7].

Some considerations which are taken into account when designing and developing security and privacy management schemes include; good performance, low power consumption, high resilience to attacks, unauthorized tampering of the data as well as end to end security. Data security mechanism in IoT offer unauthorized access to information or any other object through preventing change or deletion. Privacy schemes retain the right to direct the collected information as to its use and purpose.

To the author's knowledge, current literature studies include discussion and analysis of major IoT security- and privacy-related issues and threats [8]. Nevertheless, these works do not offer general guidelines on how an IoT system would be shielded from the surveyed threats. In addition, they do not incorporate risk evaluation in line with real systems physically deployed in the context of the smart city setting. Therefore, the main the goal of this work is aimed at such essential component as privacy practices. IoT with the help of private and protected solutions. recommendation for risk and security in IoT as well as the recommended. guidelines again depend on recent standards of the National Institute of Standards and Policies of utilizing technology, in this case, have been outlined under the NIST [9] and the GDPR privacy regulation.

Thus, the aim of this paper is to analyze some essential best practices solutions on critical key aspects:

- Data encryption that means to convert data from plaintext or unencrypted form to the ciphertext or encrypted form by offering data integrity, authenticity, and a set of services that maintains the irrevocability of a given message.
- Data anonymization for the removal of identity details for snippets data.

- To assess the security of and to gain insight into the security risk of the most evolved and sophisticated IoT environments.
- Data variety involved, the computing power of devices and cybersecurity measures available on them that regrettably are not unique and do not provide similar protection for all possible IoT versions of deployment.
- Each hardware and software element – in order to judge the risk in general and the risk of the individual links which the whole chain of the entire system [46].

Therefore, the main contribution of this paper are as follows. Here, we have described IoT privacy and security measures and a set of procedures based on recommendations by NIST and the adopted GDPR regulation. It is possible to consider the described best practices as rules for avoiding and addressing privacy and security challenges in systems related to IoT. Two actual IoT-based applications have been discussed in this paper, including a crowding monitoring system and a vehicular mobility system, with the consideration and application of the enumerated best practices to enhance security and privacy for both applications.

The rest of the paper is organized as follows: Section 2 reviews the theoretical background and related work, focusing on studies related to IoT security and privacy. Section 3 provides a comparative analysis of existing state-of-the-art approaches to IoT privacy and security. Section 4 examines Best practices Overview, Section 5 includes two real-world IoT-based applications in the context of crowding and mobility monitoring, discussing their implementation. Finally, Section 6 presents the conclusions of the study.

2. Background Study

Recently EC (The European Commission) has published a report [10] dedicated to the Features and Benefits of IoT known as the Internet of Things. The first section of the report focuses on the existing EU legislation governing safety of products intended to be on the European market. It is only important to remember that, at the moment, regulatory product safety has a number of deficiencies that are actually need to be supplemented with the help of the new legislative initiatives of the EU and the Member States. Such regulations are used all over the world. Many issues on this matter were prepared before the birth of digital technologies like artificial intelligence, IoT, or robotics and thus, the rules are quite often unable to control the sorts of risks associated with new technologies. Especially, the properties of emerging technologies can create a situation where it is unclear who is responsible for any damages, therefore, victims of accidents related to products and services, including emerging digital products, should not undergo a level of protection lower than the protection of traditional technologies. The spectrum a scenario covers, and the variety of devices in each IoT system suggest that security and privacy properties must be stronger and more adaptable.

The Previous work within the same domain was conducted aiming at addressing issues like the detection and handling of malicious or faulty nodes, protection against attack, the ability to prevent threats, and mutual authentication at runtime. malfunctioning nodes, safety against attacks, prevention of malicious threats, and dynamic mutual authentication. Yang et al. [11] proposed the most pertinent limitation of IoT devices and their solutions through categorizing IoT attacks and the discussion about the mechanism and architecture for authentication, access control, and security challenges in various IoT layers. A. R. Sfar et al. [12] discussed an IoT security roadmap recapitulated about a cognitive and systemic approach illustrating their function, how the components might interact with other central components, and their consequences on the total. An example is then described to illustrate the mechanism and cooperation of the systemic and cognitive architecture of the model. Furthermore, the assessment of security questions was made from the viewpoint of the novel taxonomy of the IoT framework and the standardization activities, so that the future research avenues could be suggested.

Tawalbeh et al.,[13], discussed of IoT privacy and solutions on challenges and solutions. The given paper critically evaluates the past background of IoT systems and their security aspects, as well as privacy policies although no practical solution for people's privacy is presented. Moreover, in addition to the legal aspects related to IoT data, there are technical aspects and no less important than the legal ones: intrusion prevention and detection in the IoT environment are becoming more and more popular in the scientific information space [14]. The main objective of the research by Rizvi et al. [15], is to extend the existing knowledge about IoT research in the following aspects: the domains where IoT is widely utilized, the security needs of current IoT, and the existing security approaches that may be proposed or implemented with their weaknesses. Security and privacy of data and things is one of the significant issues of IoT.

Zhang et al. [16], authors took into consideration authentication, authorization, identification, and localization of IoT objects and then give further discussion concerning the risks and vulnerabilities of software and backdoors probing in IoT and Android. Nevertheless, privacy is only considered to a very limited extend in the IoT and no solutions concerning the collection of the data and the anonymization of data are given.

Several studies have concentrated on particular security and privacy challenges. In reference Tariq et al. [17], a framework for Industrial Internet of Things (IIoT) is introduced, aimed at mitigating risks by identifying compromised nodes and implementing a policy enforcement mechanism to isolate them. H. M. Almohri et al. [18] outlines an anomaly detection approach that employs an architecture utilizing device proxies to regulate access to devices and gather pertinent data. This study also includes an experimental case analysis utilizing data generated from a typical IoT subnetwork environment, which lacked specific controls apart from the sensor locations. M. Zhuo et al. [19] presents a blockchain-based privacy-aware data access control (BPADAC) scheme designed for the secure and distributed sharing of Unmanned Aerial Vehicle (UAV) data within a cloud-based Internet of Drones (IOD) framework, accompanied by a formal security analysis. Nonetheless, these investigations did not address risk evaluation based on actual systems that are physically deployed within a smart city context.

Gelenbe et al. [20] proposed a distributed self-supervised federated intrusion detection algorithm (DISFIDA) for health IoT and Internet of Vehicles. This algorithm utilizes online learning to enhance security by detecting intrusions in real-time, thereby improving the resilience of IoT systems. Liu et al. [21] investigated a novel approach for secure data aggregation in IoT networks. Their method integrates encryption techniques with machine learning algorithms to detect and prevent unauthorized data manipulation, ensuring data integrity in IoT systems. The experimental results show a significant improvement in the accuracy of detecting anomalies without sacrificing computational efficiency.

Pütz et al. [22] assessed the effectiveness of IoT security best practices in protecting against threats. They developed a methodology to evaluate and rank these practices based on their impact, providing valuable insights for manufacturers to prioritize security measures effectively. Chen et al. [23] introduced a blockchain-based framework for ensuring the privacy and security of smart home devices. Their research focuses on using decentralized ledgers to control access to personal data collected by IoT devices, providing an extra layer of protection against unauthorized access and potential data breaches.

Wang et al. [24] proposed a privacy-preserving architecture for IoT-enabled healthcare systems. By leveraging differential privacy and homomorphic encryption techniques, their system ensures that sensitive health data is protected during storage and transmission. The study demonstrates that this method can balance privacy protection with the need for accurate health analytics. Gelenbe and Nakip [25] introduced an online self-supervised deep learning approach for intrusion detection systems. This method enhances the detection capabilities of IoT systems by learning from new data without requiring labeled datasets, thereby improving security over time. Zhao et al. [26] explored the use of artificial intelligence in strengthening the security of IoT networks. Their study developed a machine learning model that can predict and prevent security breaches by analyzing network traffic patterns and identifying unusual behaviors indicative of potential threats.

In this study, we endeavor to advance the current state of knowledge in the field. Initially, we identify and analyze the optimal practices for ensuring privacy and security in Internet of Things (IoT) systems. These practices encompass a series of procedures that can serve as guidelines for identifying and addressing privacy and security challenges within IoT frameworks. Subsequently, we implement the identified best practices in two practical IoT use cases. Finally, we conduct a comparative analysis of the overall risk scores of these IoT systems, as determined by our proposed methodology, against those obtained through existing state-of-the-art approaches.

3. Comparison of Existing Studies

Table 1. A Comparative Analysis of Existing Studies Addressing Privacy and Security Best Practices for IoT Solutions

Study	Focus	Proposed Method	Working of Method	Limitations
Yang et al. [11]	Security challenges and authentication mechanisms in IoT	Categorization of IoT attacks and security architectures	Provides a taxonomy of IoT attacks and outlines mechanisms for authentication, access control, and security at various layers	Limited focus on practical implementation or scalability in real-world IoT environments
A. R. Sfar et al. [12]	IoT security roadmap and systemic architecture	Cognitive and systemic security architecture	Proposes a comprehensive framework illustrating how components interact for improved security	Lacks practical demonstrations and applicability to diverse IoT use cases
Tawalbeh et al. [13]	IoT privacy policies and challenges	Critical evaluation of existing IoT privacy practices	Reviews IoT privacy background and legal aspects	Does not propose practical solutions or address user privacy implementation
Rizvi et al. [15]	IoT domains and their security needs	Analysis of existing security approaches	Examines IoT utilization domains, security needs, and existing security weaknesses	Insufficient focus on risk assessment and real-world IoT systems
Zhang et al. [16]	Authentication and	Framework for authentication and localization	Discusses risks and vulnerabilities in IoT	Limited coverage of privacy issues

	vulnerabilities in IoT		and Android, focusing on authentication and access control	and lack of solutions for anonymization of data
Tariq et al. [17]	Industrial IoT security framework	Policy enforcement mechanism for compromised node detection	Identifies compromised nodes and enforces policies to isolate them	No detailed testing in real-world industrial IoT systems
H. M. Almohri et al. [18]	Anomaly detection in IoT networks	Proxy-based anomaly detection architecture	Utilizes device proxies to monitor access and detect anomalies	Relies heavily on experimental setups, lacks scalability for larger IoT networks
M. Zhuo et al. [19]	Privacy-aware UAV data sharing	Blockchain-based privacy-aware data access control (BPADAC)	Secure and distributed sharing of UAV data in IoD using blockchain	Limited applicability beyond UAV use cases and lacks generalized risk evaluation for smart city systems
Gelenbe et al. [20]	Real-time intrusion detection in IoT	Distributed self-supervised federated intrusion detection algorithm (DISFIDA)	Uses online learning to detect intrusions and improve IoT system resilience	Tested primarily in health IoT and IoV contexts, with limited insights on other IoT applications
Liu et al. [21]	Secure data aggregation in IoT	Encryption integrated with machine learning	Combines encryption and ML for anomaly detection and data integrity	Limited exploration of scalability and cross-domain IoT data aggregation
Pütz et al. [22]	IoT security best practices	Methodology for evaluating and ranking IoT security practices	Provides a ranking system for prioritizing IoT security measures	Focuses more on evaluation, lacks actionable implementation strategies
Chen et al. [23]	Privacy and security of smart home devices	Blockchain-based access control	Employs decentralized ledgers to manage access to IoT device data	Primarily focused on smart homes, not general IoT ecosystems
Wang et al. [24]	Privacy-preserving IoT	Differential privacy and homomorphic encryption	Protects sensitive health data during storage and transmission	Challenges in balancing privacy

	healthcare systems			protection and data utility for advanced analytics
Gelenbe and Nakip [25]	Self-supervised intrusion detection	Online self-supervised deep learning approach	Enhances IoT security by learning from unlabeled data to detect and respond to intrusions dynamically	Limited real-world deployment and lacks testing across diverse IoT system architectures
Zhao et al. [26]	AI in IoT network security	Machine learning for network traffic analysis	Predicts and prevents breaches by analyzing network behavior patterns	Limited evaluation on diverse IoT systems, lacks integration with real-time IoT traffic scenarios

4. Best Practices Overview

The term best practices suggest about a collection of well-coordinated practice, procedure and policies that can be implemented anywhere. taken as a reference. Specifically, security best practice guidelines (SBPG) can be defined as the best procedure that is characterized by the best operational characteristics, and the best quality indicators [27]. The use of SBPG in the systems that were proposed in this work targets to have an understanding of the best practice to independently achieve high privacy, while at the same time, has low possibilities of being vulnerable to unauthorized access or having the information leaked. Thus, a need has arisen to draw best practices that would provide a high level of protection for personal data and provide a high level of IoT security alongside the risks that are associated with it. We proceed in the following to chart best practice for privacy and information security and align SBPG.

Best practices pertaining to privacy are increasingly aligned with global regulations that are becoming more stringent. For instance, Europe has implemented the General Data Protection Regulation (GDPR) to address privacy concerns [28]. Concurrently, in the United States, California pioneered the California Consumer Privacy Act (CCPA) [29], while other states, including Maryland, Oklahoma, Ohio, New Jersey, Florida, and Alaska, are developing a Private Right of Action (PRA). In Asia, there is a notable regulatory advancement in personal data protection, exemplified by the enactment of China's Personal Information Protection Law (PIPL) on November 1, 2021 [30]. Additionally, India introduced a new Privacy Bill in late 2021, which includes significant provisions for non-personal data protection obligations that were enacted in 2022. Conversely, best practices concerning cyber risks adhere to international guidelines. For example, issues such as gateway breaches, the criticality of IT processes, and the vulnerabilities associated with specific login credentials are universally recognized.

4.1. Internet of Things (IoT) Privacy

This section seeks to examine the privacy concerns associated with Internet of Things (IoT) technologies in relation to established privacy guidelines. The close relationship between objects and individuals results in the potential for hazardous data collection, tracking, or mapping of individuals' locations and movements through devices such as smartphones, smartwatches, social media platforms, and other intelligent devices. For example, numerous applications utilizing Bluetooth Low-Energy (BLE) technology are capable of monitoring and assessing sleep quality, while smart footwear can track running activities, record time, count steps, and map routes. Therefore, it is essential to delineate the boundaries between lawful and unlawful behaviors, with particular emphasis on the following key aspects:

- Physical considerations include the incorporation of smart chips within specific products, the environmental implications associated with these chips and their recycling processes, the establishment of supplementary network frameworks and infrastructure to support Internet of Things (IoT) applications and hardware, as well as the effects of electromagnetic fields on animal populations.
- Privacy considerations encompass user confidence and the safeguarding of individual rights concerning data collection and processing. It is imperative to establish assurances for citizens regarding the protection of their personal information, as well as to implement measures that provide optimal security for both individuals and businesses against various forms of online cyber threats.
- Aspects of standardization include the harmonization of regional standards, the establishment of open technology standards, and the facilitation of interoperability among diverse systems.

The process of datafication, which is propelled by the Internet of Things (IoT), involves the systematic collection, processing, and transmission of data. This process requires the precise identification of the relevant stakeholders, namely the data controller and the data subject [31]. Additionally, the data subject refers to the individual whose personal data is being processed, highlighting the critical importance of safeguarding the rights and privacy of this individual.

4.2. Best Practices For Privacy in IoT

Upon the initiation of personal data processing, irrespective of the specific domain of interest, local regulations mandate the execution of a preliminary analysis to evaluate the regulatory implications. This requirement is encapsulated in the principle of "data protection by design and by default," a concept that originated in the United States and Canada in 2010 and was subsequently incorporated into European legislation through the General Data Protection Regulation (GDPR) [32]. The fundamental tenets underpinning this principle are:

- The principles of lawfulness, fairness, and transparency are paramount in the handling of personal data. It is essential to refrain from engaging in any activities that may be deemed unlawful concerning personal data.
- Furthermore, the principle of purpose limitation dictates that if there is an intention to utilize personal data for a purpose that diverges from a legal obligation.
- Moreover, the principle of data minimization emphasizes the importance of collecting only the personal data that is necessary for the specified purposes.
- Accuracy: Records must explicitly delineate any subjective opinions, specifying the source of such opinions and any pertinent alterations to the foundational facts.
- Storage Limitation: It is imperative to conduct regular reviews of the information and to delete or anonymize personal data that is no longer necessary.
- Integrity and Confidentiality: It is essential to implement appropriate security measures to safeguard the personal data in your possession.

Following the initial assessment to determine adherence to the previously mentioned principles, an evaluation of the risks associated with the specific treatment is conducted. This assessment aims to implement suitable safety measures, specifically appropriate technical measures, to mitigate identified risks. Furthermore, data storage is confined to information necessary for monitoring pedestrian and vehicular activity, while maintaining integrity, functionality, and privacy through the application of encryption and pseudonymization techniques.

4.3. IoT Security Risks

While the Internet of Things (IoT) presents distinct advantages, the prevalence of cyber-attacks, ambiguity regarding optimal security measures, and the financial implications associated with implementing these measures serve as deterrents to the widespread adoption of this technology. A study by Gemalto [33] reveals that 90% of consumers express a lack of confidence in the security of IoT devices. Furthermore, the most recent State of IoT Security report highlights current trends in this domain:

A significant majority of businesses (96%) and consumers (90%) advocate for the establishment of regulations pertaining to Internet of Things (IoT) security. Furthermore, it is noteworthy that 54% of consumers possess an average of four IoT devices; however, only 14% of these individuals consider themselves to be well-informed regarding the security of such devices.

In a comparative analysis conducted by [34], which included participants from Australia, Canada, France, Japan, the United Kingdom, and the United States, several noteworthy findings emerged regarding public perceptions of connected devices. Firstly, 63% of respondents expressed discomfort with the manner in which these devices collect data about individuals and their behaviors, characterizing this practice as 'creepy.' This apprehension is further reflected in the survey results, where approximately half of the participants across various markets (53%) indicated a lack of trust in their connected devices to safeguard their privacy and manage their information respectfully.

Moreover, a significant majority, 75%, acknowledged valid concerns regarding the potential misuse of their data by external organizations without their consent. The implications of these security concerns are substantial, as they have dissuaded nearly one-third (28%) of individuals who do not currently own smart devices from making a purchase, with security apprehensions being as influential a deterrent as the cost of the devices themselves.

Despite these widespread concerns regarding security and privacy, many individuals lack the knowledge to modify device settings in a manner that could mitigate these fears. While 80% of respondents reported familiarity with setting and resetting passwords, only 50% were aware of how to disable the collection of data pertaining to users and their behaviors.

The aforementioned findings underscore the significance of user trust as a critical element in harnessing the full potential of the Internet of Things (IoT). The design of digital security has become increasingly vital for IoT devices across all components, as it is necessary to mitigate the risk of vulnerabilities in any single component compromising the overall security of the device or the system in which it operates.

4.4. Best Practices Security Risks

Security risk management in the realm of Information and Communications Technology (ICT) involves the identification of security risks and the implementation of strategies to mitigate these risks, encompassing both hardware and software/platform components [35-36]. The primary measures for risk mitigation can be categorized into three key areas: the utilization of software, the deployment of hardware, and the engagement of qualified personnel to ensure a secure operational environment against potential threats. It is essential to address security prevention measures at each layer of the OSI model, given the presence of vulnerabilities, to effectively reduce risks [37]:

- Impending threats with reference to the physical layer might lead to the denial of service resulting in unavailability of application.

- Data Link layer threats include switch security aspects such as ARP spoofing, MAC flooding and spanning tree attacks to which solutions include for example; Modifying network switch configuration.
- Network and transport layers threats can cause unauthorized retrieval of endpoint identity or unauthorized access to internal systems and could be reduced or solved by implementing Network Address Translation, Access Control Lists, or firewall technologies;
- For session and presentation layers both user and data unauthorized access can be prevented, using simple login and password or using more effective biometrics of the user [38].
- The Application layer threats encompass backdoor attacks which can be neutralized by the use of set up tools like virus scanners or web inspect.

Given that the complete eradication of risk is unattainable, best practices emphasize the importance of mitigating security risks. In reference [39], a taxonomy of Internet of Things (IoT) attacks was introduced to highlight the security vulnerabilities associated with various scenarios that target different system assets and seek to undermine specific security objectives.

The four categories of attacks examined in this paper include [46]:

1) Device: This category encompasses attacks that induce abnormal behavior in Internet of Things (IoT) systems, which may occur through various means such as manipulation of hardware ports, node tampering, malicious code injection that results in system dysfunction, the deployment of trojans, jamming techniques, or unauthorized remote firmware updates.
2) Infrastructure: This type of attack focuses on the "back end" of a system, specifically the data access layer, which includes data storage and processing. Such attacks pose a threat to the physical integrity and availability of data or devices situated at the network's edge.
3) Communication: This category pertains to attacks that disrupt the exchange of data among IoT devices, thereby jeopardizing communication technologies, standards, protocols, and channels. It also encompasses vulnerabilities within the network layer, including switching, routing, and associated protocols.
4) Service: This category addresses service-oriented attacks that exploit the inherent functionalities of a system, particularly at the application layer. It includes phishing attacks, social engineering tactics, control hijacking, the use of malicious scripts, cryptanalysis attacks, exploitation of buffer overflow vulnerabilities, and any attempts to extract sensitive information from applications.

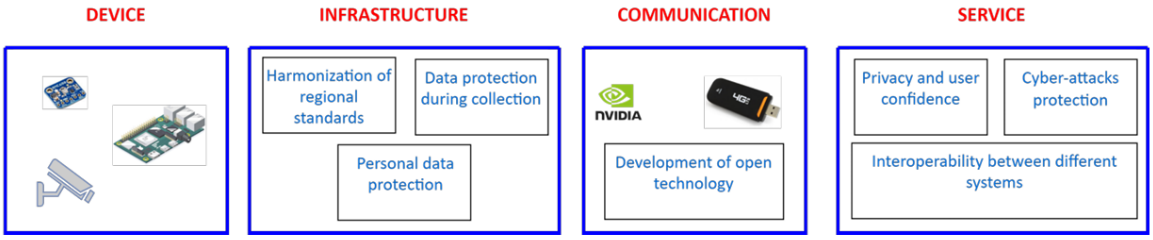

DEVICE
INFRASTRUCTURE
Harmonization of regional standards
Data protection during collection
Personal data protection
COMMUNICATION
NVIDIA
Development of open technology
SERVICE
Privacy and user confidence
Cyber-attacks protection
Interoperability between different systems

Figure 1. Taxonomy for Risk Management. Reproduced from [46]

The Risk management encompasses a variety of elements across several phases. The devices employed, ranging from sensors to commercial-grade electronics, significantly influence privacy and cybersecurity concerns. Essential factors to consider include the operational environment of the system, methods of data storage (such as cloud services, servers, and data centers), and the design of infrastructure to comply with regional standards. The safeguarding of data during the acquisition process is frequently neglected due to which personal data is subject to regional regulations. Furthermore, advancements in telecommunications enhance accessibility, integration, and interoperability. Contemporary services must strive to achieve a balance between user trust, data security, and cybersecurity measures to effectively mitigate cyber threats.

The responsibilities associated with data management are contingent upon whether the data is safeguarded by suitable software, which is typically the responsibility of the customer, or whether the cloud service provider is deemed responsible for the underlying infrastructure. It is important to recognize the numerous connection ports associated with specific services that adhere to established standards, such as UDP or TCP. This includes well-known ports (22/TCP for SSH), registered ports (1194/UDP for OpenVPN), unregistered ports (5800/TCP for VNC), and dynamic ports (49152 to 65535). Consequently, each of these stages presents critical challenges and potential vulnerabilities that may pose varying degrees of risk to the effective operation of a system, and in severe cases, may lead to the compromise of sensitive data that can be traced back to individuals.

5. Best Practices Implementation

This section delineates two practical Internet of Things (IoT) use cases to illustrate the primary steps necessary for effectively securing a system in alignment with the best practices outlined in Section IV. The structure of this section is organized as follows: Subsection V-A offers a brief description of the two use cases, while Subsection V-B presents an overview of the key decisions made to secure the systems in accordance with the established best practices.

5.1. Real Use Cases

The discussed systems concern the monitoring of the flow of people and vehicles in smart cities. The flow of people is a particularly relevant issue, especially because of the recent health emergency that is affecting the entire world population. The monitoring of these flows involves both indoor spaces and large outdoor events. Moreover, the monitoring of pedestrian flows allows the statistical analysis and the determination of origin-destination matrices that can be treated and studied for the optimization of bus frequencies of urban mobility services. Therefore, the pedestrian flow is closely related to the vehicular flow. Its monitoring and control allow flexible, dynamic, and real-time management of vehicular flows. Both systems have been installed in the city of Cagliari (Sardinia, Italy) and take as input the detection of smartphones and vehicle license plates, which are discussed in more detail in the following subsections.

5.1.1. *Crowding Monitoring Sub-System*

The Wi-Fi standard has emerged as a fundamental technology for connecting portable devices, including smartphones, tablets, and various wearable technologies. Its widespread adoption among smartphones can be attributed to its ability to facilitate Internet connectivity in numerous locations, bolstered by the increasing availability of hotspots and open wireless networks. Regardless of their active status, Wi-Fi radio interfaces transmit data packets that include a unique Media Access Control (MAC) address, which can often be linked to the specific address of the device's network interface card. This approach for detecting individual presence and tracking their movements is referred to as Wi-Fi tracking. MAC addresses are intentionally designed to be persistent and globally unique, serving as the physical address for the network interfaces of mobile devices. These addresses are transmitted within MAC frames alongside additional information necessary for the maintenance of network infrastructure. This review focuses on the use of Wi-Fi tracking to gather such insights and does not propose any specific system or solution.

In light of this information, various approaches have been developed to monitor attendance in designated areas. One such approach involves utilizing an external network card connected to a Raspberry Pi device to intercept Wi-Fi traffic from mobile devices by analyzing their MAC addresses. A key feature of these crowd monitoring systems is the ability to prevent the repeated counting of previously recorded MAC addresses. It operates effectively within a maximum range of approximately 50 meters and is applicable in both indoor environments (such as monitoring occupancy within buses or rooms) and outdoor settings (for instance, tracking individuals near traffic signals). A practical application of this technology includes the detection of smartphone users on public transportation, such as buses or trains. A proof of concept was conducted and evaluated in the city of Cagliari, where the devices were installed in two specific locations [46]:

- Onboard public transport vehicles
- At fixed points near public transport stops

Upon establishing the network and power connections, all devices were tasked with transmitting the processed data to a dedicated Internet of Things (IoT) platform designed specifically for the processing and management of information originating from the urban environment. The data was transmitted post-processing, necessitating the acquisition of data, execution of on-board processing utilizing anonymization techniques, and subsequent transmission of the anonymized data to ensure the protection of privacy.

5.1.2. *Mobility Monitoring Sub-System*

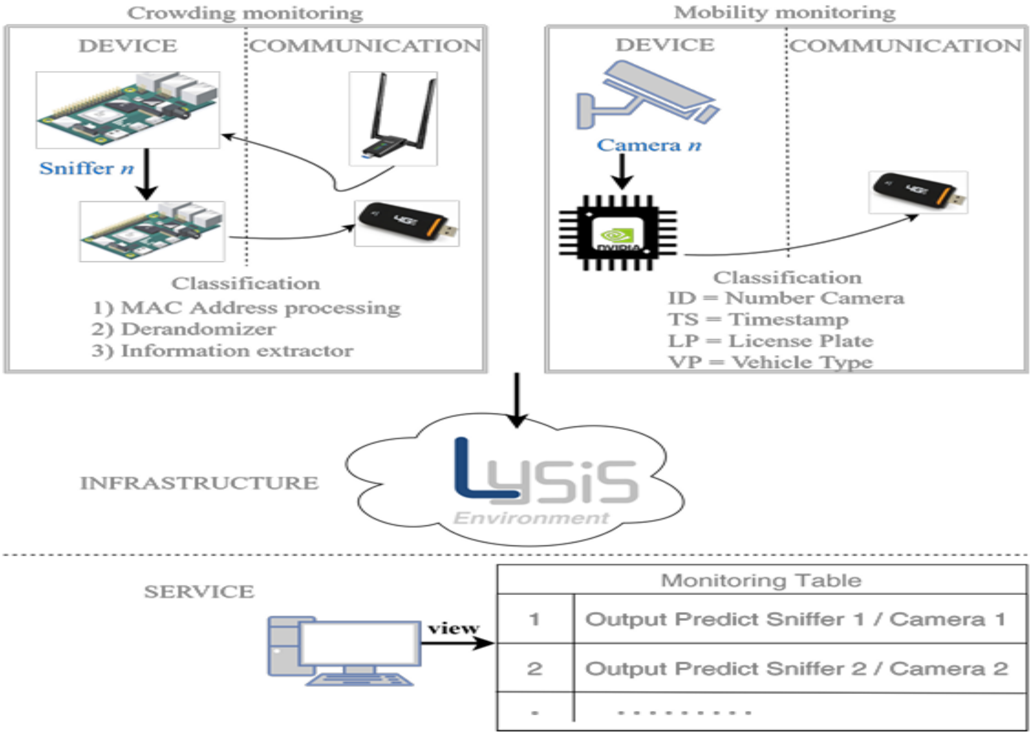
The vehicle tracking component of mobility monitoring has been explored using techniques similar to those employed in crowd monitoring, focusing on the identification of both the vehicle type and its specific identification through license plates. Studies in this domain have utilized a network of strategically positioned cameras to monitor road intersections and traffic circles. These cameras function as image and video acquisition sensors, capable of operating effectively under various weather conditions and during both daytime and nighttime. The cameras are interconnected through an Ethernet link to an NVIDIA Jetson NX processing unit, which executes the following operations [46]:

1) the processing unit receives images of the license plates as input;
2) a numerical conversion is conducted utilizing a neural network known as Automatic License Plate Recognition (ALPR).
3) an irreversible anonymization algorithm is subsequently applied, which assigns a Hash to each license plate, thereby preventing the original license plate from being traced.

The mobility monitoring subsystem depicted in Figure 2 illustrates a vehicle detection system comprising multiple levels of operation. The cameras continuously capture video footage, focusing on the rear of vehicles traversing a designated gate or roadway. The Automatic License Plate Recognition (ALPR) algorithm is responsible for converting the captured image into an alphanumeric string that represents the sequence of characters on the identified license plate. This string serves as the input for the Hash algorithm, which transforms the license plate data into a 512-bit string through a pseudorandom process. The resulting anonymized data is temporarily held in volatile memory, aggregated with other anonymized data, and subsequently transmitted via LTE once a sufficiently sized buffer is achieved. The proposed system transmits anonymized data to a database (DB) integrated within a Social Internet of Things (SIoT) platform known as Lysis. This platform facilitates the reprocessing of data to generate statistical analyses on an hourly, daily, monthly, and yearly basis. Lysis is specifically designed for distributed IoT applications that involve socially connected objects [40].

5.2. Implementation of Best Practices

This subsection delineates the methodologies employed for data protection following acquisition. Sensitive data is subjected to pre-processing, wherein it is transformed into a Hash key utilizing specialized Hash functions that are appropriate for encryption purposes [41]. These functions produce fixed-size, unidirectional Hash values, thereby complicating reverse-engineering efforts, which can only be achieved through brute-force or rainbow table attacks. While Hash functions improve the efficiency of data retrieval, their effectiveness diminishes with a reduced number of entries. To uphold privacy, comprehensive data protection measures are instituted throughout the stages of acquisition, processing, transmission, and storage.



Monitoring Table	
1	Output Predict Sniffer 1 / Camera 1
2	Output Predict Sniffer 2 / Camera 2
-	. . . .

Figure 2. Taxonomy for pedestrian and vehicular detection system [46]

5.2.1. *Privacy*

Privacy is associated with information that is intrinsically significant or sensitive to individuals. In the context of this discussion, the MAC address of a smartphone and the license plate of a vehicle are clearly identifiable pieces of information linked to specific individuals. Table 2 presents a summary of the primary algorithms that were examined.

Table 2. Anonymization Algorithms. Reproduced from [46]

Algorithm Name	Advantages	Disadvantages
SHA-512 [42]	Best security level between the options	Computational costs higher than SHA-256 "double"
SHA-256 "double" [43]	Good level of security	High computational costs
MD5 [44]	Lower computational cost of the three	Not safe enough; they increase collisions

The Secure Hash Algorithm (SHA) family, which includes SHA-256, SHA-384, and SHA-512, is categorized under the MD family of hash functions [43]. The SHA-256 algorithm operates by processing the input message twice using a consistent anonymization technique. SHA-512 [45] is designed to hash a message M, which can have a length of k bits, where k ranges from 0 to 2^128. This algorithm represents the third generation of cryptographic hash functions developed by the National Institute of Standards and Technology (NIST) and is founded on principles distinct from those of SHA-256. It employs a construction known as SPONGE, which enhances its resistance to potential cryptanalytic attacks that may affect SHA-256. Currently, SHA-512 is regarded as secure, with no significant vulnerabilities identified. Although SHA-3 was introduced subsequent to SHA-2, its adoption has not yet reached the levels of SHA-256, although its usage is gradually increasing. The SHA-512 algorithm operates through a three-step process [46]

a) it utilizes a message schedule comprising eighty 64-bit words
b) it employs eight working variables, each 64 bits in size
c) it generates a hash value consisting of eight 64-bit words

The output of the SHA-512 algorithm is a 512-bit message digest. Additionally, the fifth version of the MD algorithm, known as MD5, has been evaluated. The output of the MD5 algorithm is significantly shorter than that of SHA-256 and SHA-512, consisting of only 32 characters. Consequently, it is more susceptible to brute-force attacks, which increases the likelihood of successful decryption. Furthermore, MD5 is associated with a higher incidence of collisions during the hashing process. A collision occurs when two distinct input values yield the same output string from a hash function. The frequency of collisions in MD5 is considerably greater than that observed in SHA-256 and SHA-512, thereby elevating the risk of compromising sensitive data and diminishing the uniqueness of the hash outputs.

Level 3 of the mobility monitoring sub-system, as illustrated in Figure 2, transmits various data regarding the analyzed vehicles to the cloud. The SHA-512 hashing algorithm can be utilized in relation to license plates to ensure data integrity and security. The following are several potential applications of SHA-512 in conjunction with license plates:

- License Plate Verification: Each license plate can be hashed using SHA-512 to produce a unique identifier or checksum. This hashed value can subsequently be employed for verification purposes, thereby confirming that the license plate information remains unaltered and has not been subject to tampering.

- Secure Database Storage: In the context of storing license plate data within a database or system, the license plate numbers can be hashed with SHA-512 prior to storage. This practice enhances the protection of the actual license plate numbers' privacy.

- Authentication and Access Control: SHA-512 can be integrated into authentication systems that utilize license plate information as an identifier. For instance, in automated toll collection systems or parking access control mechanisms, the license plate number can be hashed and subsequently compared against a stored hash to determine access permissions.

- Secure Communication: When transmitting license plate data across a network or between systems, SHA-512 can be employed to generate a hash of the data for purposes of authentication and integrity verification.

The application of the SHA-512 hashing algorithm to license plate data enhances security by providing an additional layer of protection, thereby safeguarding the integrity and confidentiality of the information. The application of SHA-512 in conjunction with MAC addresses can be advantageous in various contexts to enhance data integrity and security. The following outlines several potential use cases for the implementation of SHA-512 with MAC addresses:

• Data Integrity: The hashing of MAC addresses using SHA-512 generates a fixed-length, unique identifier for each address. This hash serves as a mechanism to verify the integrity of the MAC address, ensuring that it remains unaltered during transmission or storage.

• Anonymization: In scenarios where privacy is paramount, anonymizing MAC addresses may be necessary. By employing SHA-512, a hashed representation of the MAC address can be produced, effectively concealing the original address while still permitting identification and matching when required.

• Access Control: In secure environments, SHA-512 can facilitate the authentication and authorization of devices based on their MAC addresses. The MAC address can be hashed and subsequently compared to pre-existing hash values to determine access rights to a network or specific resources.

- Data Storage and Lookup: Utilizing SHA-512 for the storage of MAC addresses within databases or systems can enhance the privacy of the original addresses.

Consequently, from a privacy standpoint, suitable privacy policies have been implemented to safeguard individuals without necessitating explicit consent.

6. Security Risks

The discussed system undergoes a comprehensive methodology that evaluates cybersecurity and associated risks in accordance with the NIST guidelines [9]. Each component within the system requires specific arrangements to ensure a robust level of security against data loss/tampering. The elevated level of protection attained is characterized by three primary aspects, which are elaborated upon below:

A critical aspect to be assessed is the risk scenario, particularly in relation to tampering, equipment theft, or the potential for unauthorized physical connections to external devices. Firstly, these systems are situated within the jurisdiction of the Port System Authority of the Sea of Sardinia, in locations that are not easily accessible, mounted on poles at heights ranging from 5 to 7 meters above ground level. Secondly, the area is under comprehensive video surveillance, which provides an additional layer of security for the hardware associated with the sniffing and vehicular monitoring systems.

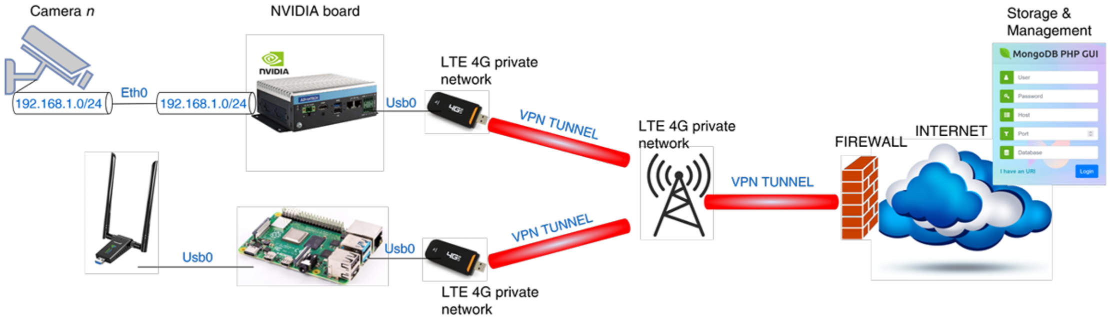


Figure 3. Implementation of practical best practices and evaluation of cybersecurity measures[46]

- Connection of modules: The hardware/software system is comprised of multiple interconnected modules, each of which plays a significant role in the overall functionality and security of the system. Different types of information transmission mediums are utilized, including both wireless and wired options, as well as public and private networks, with or without firewalls to ensure appropriate information filtering. In the two systems under consideration, the connection between the sensor and the acquisition board is established through wired means, specifically utilizing Ethernet with private IP addressing and USB connections.

A Virtual Private Network (VPN) is a technological solution that facilitates the establishment of a secure and encrypted connection between a device and the Internet. When a VPN is employed, Internet traffic is directed through the VPN server, which encrypts the transmitted data and conceals the user's IP address. This process significantly complicates the ability of third parties, including hackers, advertisers, and governmental entities, to monitor online activities. There are several prevalent motivations for utilizing a VPN, including:

- Privacy: Virtual Private Networks (VPNs) enhance user privacy by encrypting internet traffic and concealing the user's IP address.

- Security: VPNs contribute to the security of online activities, especially when utilizing public Wi-Fi networks, which are frequently vulnerable to security threats.

- Access to restricted content: VPNs facilitate access to websites and content that may be limited or prohibited in specific geographical locations or countries.

- Circumventing censorship: VPNs enable users to bypass internet censorship and restrictions enforced by governmental authorities or Internet Service Providers (ISPs).

- Remote access: Virtual Private Networks (VPNs) facilitate remote access to an organization's network and resources from locations outside the physical office environment, while also ensuring secure connectivity to remote servers or devices.

When selecting a VPN service, it is crucial to opt for a reputable provider that maintains a strict no-logging policy and refrains from selling user data. It is also noteworthy that the utilization of a VPN may result in a reduction in internet speed, attributable to the extra processing involved in the encryption and decryption of data.

The policies governing the back-end operations dictate that incoming traffic to the cloud, and subsequently to the database, is subject to a final verification process conducted by a firewall. This firewall is responsible for monitoring incoming traffic in accordance with a predefined set of security protocols, which determine whether specific events are permitted or denied. Inadequate configuration of the firewall may result in the inadvertent allowance of traffic from any commercial 4G LTE connection. To mitigate this risk, best practices advocate for the utilization of a private 4G network segment rather than relying on commercial 4G communications. Furthermore, it is imperative that cloud data storage incorporates a five-factor authentication process for both read and write operations, which includes the user, password, host (private IP), port, and database name.

The rigorous application of the aforementioned three principles guarantees a substantial level of security and a minimal risk index. The implemented measures facilitate the encryption of the collected data and its transmission over a secured private network, thereby achieving an optimal security index at the network level. The architecture of the subsystems is illustrated in Figure 3. The cameras are interfaced with the NVIDIA video card via an Ethernet connection, utilizing private network addresses within the range of 192.168.1.0/24. A USB 4G drive is directly connected to a USB port on the NVIDIA video card, which has been configured to operate a VPN tunnel network. Data traffic is transmitted over a private 4G network segment, which is recognized by the 4G network and the firewall that permits inbound connections to the cloud where the database is hosted. A comparable approach is employed in the pedestrian monitoring system, where a dual USB Wi-Fi antenna and a USB 4G drive are connected to a Raspberry Pi board, also configured with a VPN tunnel network.

Table 3. Pedestrian system status of devices and interfaces [46]

Component	Interfaces	Status
Wi-Fi dual antenna	USB	Enabled
Raspberry Pi 4 B+	Ethernet	Disabled
	USB1	Enabled (dual Wi-Fi antenna)
	USB2	Disabled
	USB3	Disabled
	USB4	Disabled
	Bluetooth radio interface	Disabled
	Wi-Fi radio interface	Disable
	Raspi OS Login	Psw 12 alphanumeric

		+ symbols elements
LTE USB	USB	enabled
LTE connection	4G private network + tunnel VPN	enabled
Firewall	LTE private traffic seg mentation	enabled
Link VM- MongoDB	Root ssh	User ********* Password ****** Host **.***.**.*** Port "xyzty "

Table 4. Vehicular system status of devices and interfaces [46]

Component	Interfaces	Status
GIFRAN camera	Ethernet only	Enabled
Link GIFRAN Camera	Ethernet	Enabled
NVIDIA Board	Ethernet	Enabled
	USB 1 USB 2 USB 3	Enabled (usb 4G LTE) x x
NVIDIA Board	Operating system access	Psw 12 alphanumeric + symbols elements
LTE USB	USB	Enabled
LTE connection	4G private network + tunnel VPN	Enabled
Firewall	LTE private traffic segmentation	Enabled
Link VM- MongoDB	Root ssh	User ********* Password ****** Host **.***.**.*** Port "xyzty "

Each sniffer and vehicular monitoring system is equipped with a 4G SIM card operating within a private network segment. Notably, no wireless Wi-Fi connections are utilized in the described system. On both the NVIDIA board and the Raspberry Pi, only those processes essential for the fundamental operations have been maintained, while superfluous or non-essential processes have been terminated. Tables 3 and 4 provide a summary of the status of the interfaces involved in the pedestrian and vehicular traffic monitoring systems. These two systems, which are based on distinct data acquisition approaches, are interconnected through the transmission of data over a private LTE network and VPN tunnel.

7. Conclusion

Security and privacy concerns represent significant challenges within the Internet of Things (IoT) landscape, an area that has been inadequately addressed in existing literature, particularly in relation to actual IoT systems and applications. This paper provides a comprehensive review of best practices for addressing these challenges, guided by established frameworks such as the National Institute of Standards and Technology (NIST) guidelines and the European General Data Protection Regulation (GDPR). It explores two illustrative use cases: one focusing on crowd monitoring and the other on vehicular mobility. These use cases highlight how existing procedures and guidelines, rooted in best practices, can be applied to reduce privacy and security vulnerabilities in IoT systems. Future research endeavors will explore a variety of IoT applications to further underscore the importance of integrating the proposed best practices in the design of IoT systems to diminish the incidence of security and privacy challenges. Additionally, alternative evaluation methodologies may be explored and proposed, necessitating adaptation in response to ongoing advancements in technology and regulatory frameworks.

References

1. B. Jovanovic. (2022) Internet of Things statistics for 2022- Taking Things Apart. [Online]. Available: "https://dataprot.net/statistics/iot-statistics/"
2. Paloalto. (2020) 2020 Unit 42 IoT Threat Report. [Online]. Available: https://iotbusinessnews.com/download/white-papers/UNIT42 IoT-Threat-Report.pdf
3. M.Fadda, M.Anedda, R.Girau, G.Pau, and D.D.Giusto, "A Social Internet of Things Smart City Solution for Traffic and Pollution Monitoring in Cagliari," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2373–2390, 2023.
4. A. Floris, R. Girau, S. Porcu, G. Pettorru, and L. Atzori, "Implementation of a Magnetometer based Vehicle Detection System for Smart Parking applications," in 2020 IEEE International Smart Cities Conference (ISC2), 2020, pp. 1–7.
5. T. A. Ahanger, A. Aljumah, and M. Atiquzzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," Computer Networks, vol. 206, p. 108771, 2022.
6. P. M. Chanal and M. S. Kakkasageri, "Security and Privacy in IoT: A Survey," Wireless Personal Communications, vol. 115, no. 2, pp. 1667 1693, 2020.
7. M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," Computer Science Review, vol. 38, p. 100312, 2020.
8. N. Chaurasia and P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in IoT," e-Prime- Advances in Electrical Engineering, Electronics and Energy, vol. 4, p. 100158, 2023.
9. NIST. (2022) National Institute of Standards and Technology- NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations". [Online]. Available: "https://www.nist.gov/"
10. European Union, "Report from the commission to the european parliament, the council, the european economic and social committee: Report on the safety and liability implications of artificial intelligence, the internet of things and robotics- 19.2.2020." 2020, p. 64.
11. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.
12. A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, vol. 4, no. 2, pp. 118–137, 2018.
13. L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider., "IoT Privacy and Security: Challenges and Solutions," Applied Sciences, vol. 12, p. 4102, 2020.
14. C. A. d. Souza, C. B. Westphall, R. B. Machado, L. Loffi, C. M. Westphall, and G. A. Geronimo, "Intrusion detection and prevention in fog based IoT environments: A systematic literature review," Computer Networks, vol. 214, p. 109154, 2022.
15. S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT," in 2018 17th IEEE Int. Conf. On Trust, Security And Privacy In Computing And Communications/ 12th IEEE Int. Conf. On Big Data Science And Engineering (TrustCom/Big DataSE), 2018, pp. 163–168.
16. Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," in 2014 IEEE 7th Int.Conf. on Service-Oriented Computing and Applica tions, 2014, pp. 230–234.
17. U. Tariq, A. O. Aseeri, M. S. Alkatheiri, and Y. Zhuang, "Context-aware autonomous security assertion for industrial IoT," IEEE Access, vol. 8, pp. 191785–191794, 2020.
18. H. M. Almohri, L. T. Watson, and D. Evans, "An attack-resilient archi tecture for the Internet of Things," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3940–3954, 2020.
19. M. Zhuo and J. Zhang, "Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-based IoD Systems," IEEE Access, vol. 11, pp. 45206– 45221, 2023.

20. E. Gelenbe, B. C. Gül, and M. Nakıp, "DISFIDA: Distributed Self-Supervised Federated Intrusion Detection Algorithm with Online Learning for Health Internet of Things and Internet of Vehicles," *Internet of Things*, vol. 17, p. 100453, Dec. 2024.
21. H. Liu, Y. Zhang, L. Li, and L. Wang, "Secure Data Aggregation in IoT Networks Using Encryption and Machine Learning," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 2934–2945, 2024.
22. P. Pütz, R. Mitev, M. Miettinen, and A.-R. Sadeghi, "Unleashing IoT Security: Assessing the Effectiveness of Best Practices in Protecting Against Threats," *arXiv preprint arXiv:2308.12072*, Aug. 2023.
23. S. Chen, X. Li, X. Wang, and L. Zhang, "Blockchain-Based Framework for Ensuring Privacy and Security of Smart Home Devices," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 7, pp. 4571–4580, 2023.
24. F. Wang, X. Zhang, Z. Li, and Y. Song, "A Privacy-Preserving Architecture for IoT-Enabled Healthcare Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, pp. 1123–1135, 2022.
25. E. Gelenbe and M. Nakip, "Online Self-Supervised Deep Learning for Intrusion Detection Systems," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 5668–5683, 2024.
26. Y. Zhao, X. Liu, and H. Zhang, "Artificial Intelligence for Security in IoT Networks: A Machine Learning Approach," *International Journal of Network Security*, vol. 23, no. 1, pp. 52–64, 2021.
27. M. G. Samaila, C. Lopes, E. Aires, J. B. F. Sequeiros, T. Simoes, M. M. Freire, and P. R. M. Inácio, "A Preliminary Evaluation of the SRE and SBPG Components of the IoT-HarPSecA Framework," in 2020 Global Internet of Things Summit (GIoTS), 2020, pp. 1–7.
28. GDPR. (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Online]. Available: "https://eur lex.europa.eu/eli/reg/2016/679/oj"
29. CCPA. (2021) California Consumer Privacy Act (CCPA) State of California- Department of Justice. [Online]. Available: "https://oag.ca.gov/privacy/ccpa"
30. PIPL. (2021) The PRC Personal Information Protection Law. [On line]. Available: "https://www.china-briefing.com/news/the-prc-personal information-protection-law-final-a-full-translation/"
31. D. Walentek, "Datafication process in the concept of smart cities," Energies, vol. 14, no. 16, p. 4861, 2021.
32. Gemalto. (2017) Gemalto survey confirms that Consumers lack confidence in IoT device security. [Online]. Available: https://www6.gemalto.com/state-of-iot-security-2017-press-release
33. B. Trust. (2019) The Trust Opportunity: Exploring Consumer Attitudes Available: to the Internet of Things. [Online]. https://www.internetsociety.org/resources/doc/2019/trust opportunity-exploring-consumer-attitudes-to-iot/
34. L.Babun, K.Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: Communication, security, and privacy perspectives," Computer Networks, vol. 192, p. 108040, 2021.
35. S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," Computer Networks, vol. 191, p. 108005, 2021.
36. P. Ruiu, A. Lagorio, M. Cadoni, and E. Grosso, "Enhancing e-id card mobile-based authentication through 3d facial reconstruction," Journal of Information Security and Applications, vol. 77, p. 103577, 2023.
37. G. L. Masala, P. Ruiu, and E. Grosso, "Biometric authentication and data security in cloud computing," Computer and network security essentials, pp. 337–353, 2018.
38. C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies," IEEE Internet of Things Journal, vol. 9, no. 1, pp. 199–221, 2021.
39. R. Girau, S. Martis, and L. Atzori, "Lysis: A Platform for IoT Distributed Applications Over Socially Connected Objects," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 40–51, 2017.

40. J. Wang, W. Liu, S. Kumar, and S. Chang, “Learning to Hash for Indexing Big Data—A Survey,” Proceedings of the IEEE, vol. 104, no. 1, pp. 34–57, 2016.
41. NIST. "Hash (2017) Functions NIST | SP CSRC”. 800-106 [Online]. SHA-512 Available: "https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards and Guidelines/documents/examples/SHA512.pdf"
42. H. Gilbert and H. Handschuh, “Security analysis of sha-256 and sisters,” in Selected Areas in Cryptography, 2004, pp. 175–193.
43. W. ZheLong, D. Yan, W. Qing, L. XiJian, and G. Liang, “Research on software comparison of electric energy data acquire terminal based on MD5algorithm,” in 2017 Chinese Automation Congress (CAC), 2017, pp. 845–849.
44. Q. Wang, X. Lu, C. Zhang, Y. Yuan, and X. Li, “LSV-LP: Large-scale video-based license plate detection and recognition,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 1, pp. 752–767, 2022.
45. Y. Gao, H. Lu, S. Mu, and S. Xu, “Group Plate: Toward Multi-Category License Plate Recognition,” IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 5, pp. 5586–5599, 2023.
46. M. Anedda, A. Floris, R. Girau, M. Fadda, P. Ruiu, M. Farina, A. Bonu, and D. Giusto, “Privacy and Security Best Practices for IoT Solutions,” IEEE Access, vol. 4, pp. 123–130, 2016.