Journal of Computer and Communications, 2023, 11, 26-42
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Security and Privacy Concerns over IoT Devices Attacks in Smart Cities (2022)

Azizi Majid

Independent Researcher, Wuhan, China
Email: sys_net2005@yahoo.com

How to cite this paper: Majid, A. (2023) Security and Privacy Concerns over IoT Devices Attacks in Smart Cities (2022). *Journal of Computer and Communications*, **11**, 26-42.
https://doi.org/10.4236/jcc.2023.111003

Received: October 28, 2022
Accepted: January 17, 2023
Published: January 20, 2023

Abstract

Due to the long-term goal of bringing about significant changes in the quality of services supplied to smart city residents and urban environments and life, the development and deployment of ICT in city infrastructure has spurred interest in smart cities. Applications for smart cities can gather private data in a variety of fields. Different sectors such as healthcare, smart parking, transportation, traffic systems, public safety, smart agriculture, and other sectors can control real-life physical objects and deliver intelligent and smart information to citizens who are the users. However, this smart ICT integration brings about numerous concerns and issues with security and privacy for both smart city citizens and the environments they are built in. The main uses of smart cities are examined in this journal article, along with the security needs for IoT systems supporting them and the identified important privacy and security issues in the smart city application architecture. Following the identification of several security flaws and privacy concerns in the context of smart cities, it then highlights some security and privacy solutions for developing secure smart city systems and presents research opportunities that still need to be considered for performance improvement in the future.

Keywords

Smart Cities, Internet of Things (IoT), Security, Privacy, Attacks, Threats

1. Introduction

Due to its stringent standards and practical basis in an urbanized setting, the idea of a "smart city" has received far too much attention from business and academia. In general, "smart cities" refer to the application of technology-based solutions to raise a community's standard of living, facilitate better communication with the government, and encourage sustainable growth [1] [2]. Smart cities

are developed to enhance social and urban interconnectivity [3]. Smart cities balance and connect social, environmental, and economic development variables through decentralized processes to better manage essential resources, urban flows, and real-time activities [4]. According to research from the United Nations Population Fund, more than 50% of people worldwide live in urban areas, and it is anticipated that this number will increase to 70% in 30 years [5]. A highly rising number of cities globally have started to build their smart strategies to enhance citizen well-being, boost economic growth, and administer contemporary cities sustainably and intelligently. In 2017, Cisco announced a $1 billion investment to develop smart, affordable, scalable, and inventive solutions to address urbanization and smart city issues [6].

A city's infrastructure is undoubtedly equipped with many devices that can benefit all residents. These intelligent devices are applied in areas such as homes known as smart homes, energy management, traffic control, healthcare, and transportation. A smart city uses various techniques such as cloud computing, electronics, networking, sensors, machine learning, and data mining to enable the collaboration and interaction of different components of smart cities with the network architecture [7]. Due to the vulnerabilities to various security threats present in each layer of a smart system, smart city systems and applications development may also present many security, privacy and cyber-related challenges. The current IoT devices, responsible for collecting data from various sources and delivering it to storage facilities over the existing networks, create a surface vulnerable to attacks and can be used as an entry point by malevolent attackers trying to infiltrate the system. For instance, while manipulating sensor data, malevolent attackers may provide data/information that is misleading, resulting in the loss of control over highly intelligent systems [8]. The cities also contain many pervasive Video surveillance systems and GPS for obtaining susceptible data that hackers could use to trace a person's identity and threaten their privacy. IoT devices have higher security and privacy threats than traditional networks because of their heterogeneity, scalability, and dynamic nature. These difficulties drive an overview of the currently used and developing technologies for defending smart cities and an effort to provide readers with potential research prospects for further exploration of the topic.

2. Related Studies

Many notable research surveys and reviews have been published, highlighting the concerns regarding the privacy and security of IoT smart Systems. However, not in all layers of the smart systems, as will be discussed in this paper. The existing surveys also do not identify the privacy and security solutions for IoT smart system designs. Similarly, some studies only focus on possible solutions to fix security and privacy issues. The same goes for research that considers potential fixes for security and privacy problems. According to the authors [9], most of the security measures, including encryption, biometrics, and anonymity, that are already widely used in smart cities are ineffective in protecting the security

and privacy of data. The results are from the vast amounts of data that smart city applications gather, store, and continuously evaluate. Only simple cryptographic approaches can be used in a smart city scenario because most sensors and equipment have little computational power [9]. According to the authors [10], it is crucial to design systems that interfere with the residents' privacy rights due to the introduction of some sophisticated attacks like cold boot attacks and side-channel attacks.

Research paper [11] has outlined concerns over the security and privacy of IoT systems. The article addresses a wide range of risks to generalized security and privacy in addition to spotlighting a few IoT security and privacy concerns, such as the privacy of the user, protection and authentication of data, authorization, and controlled access. The authors of [12] discuss some issues with the security and privacy of smart home devices and propose an SDN-based security mechanism for the network layer to monitor and control each IoT device's network activity. In contrast, research [13] addresses the security and unaddressed research issues associated with communication protocols for IoT.

A. Contributions of this Study

In this study, we will try to figure out why IoT systems face more security and privacy concerns than traditional computer networks, as well as the outstanding research issues surrounding the security of IoT smart devices. In addition to providing a thorough analysis of the security and privacy concerns in smart cities, this study proposes a methodology for classifying recent and upcoming innovations in this cutting-edge field. Two main contributions to the paper are 1) Examining current security and privacy issues for IoT Systems in smart cities. 2) Identifying the security and privacy requirements to counter threats of systems in smart cities and identifying the open issues and challenges that can be used to provide better solutions as a future direction. Additional research is required to identify the essential and unresolved open issues; the paper also examines the similarities and differences between these solutions that have not been discussed in the literature. **Table 1** below highlights the gaps in IoT System Security and privacy from the existing research that this study will cover.

Table 1. Gaps in existing research.

Existing Studies	Consolidated Introduction	Illustration of threats and issues at the layers of IoT	Examples of Security and privacy attacks	In-depth research on security Requirements	Suggestions for future directions
[9]	✓	✓	✓		✓
[11]	✓			✓	✓
[12]	✓	✓	✓	✓	
[13]	✓		✓		✓
[14]	✓		✓		✓
[15]	✓	✓		✓	✓
This work	✓	✓	✓	✓	✓

B. Organization of the paper

The remainder of this journal article organized as follows: The IoT design and implementation in smart cities are briefly described in Section III. Section IV discusses the security and privacy threats of IoT smart applications and the crucial security requirement considered for creating a safe and secure smart city. Section V examines the most modern security and privacy solution technologies used in smart cities and the challenges and potential opportunities to be explored in the future. Section VI, which summarizes the study, also concludes the research paper.

3. Background of IoT

A. Architecture for IoT Systems for Smart Cities

Several different architectures have been developed to maintain the growth of smart cities [14]. Since no architecture is uniform for IoT and this study proposes to clarify security and privacy issues in smart cities, we utilized a four-layered IoT architecture suggested by [15] for this study, as illustrated in **Figure 1** herein (**Figure 2**).

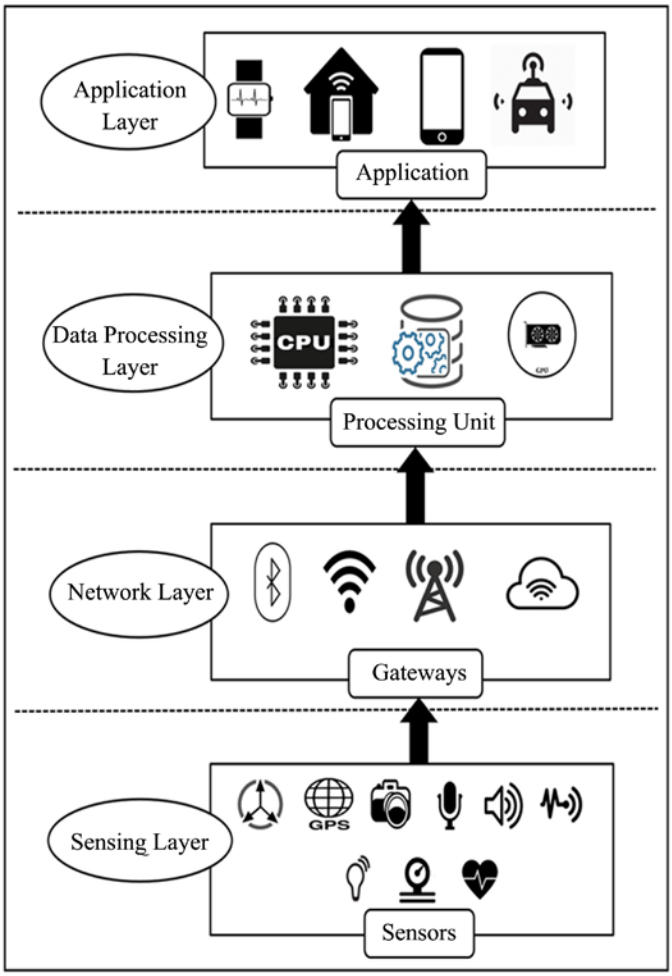

Figure 1. Layers of IoT.

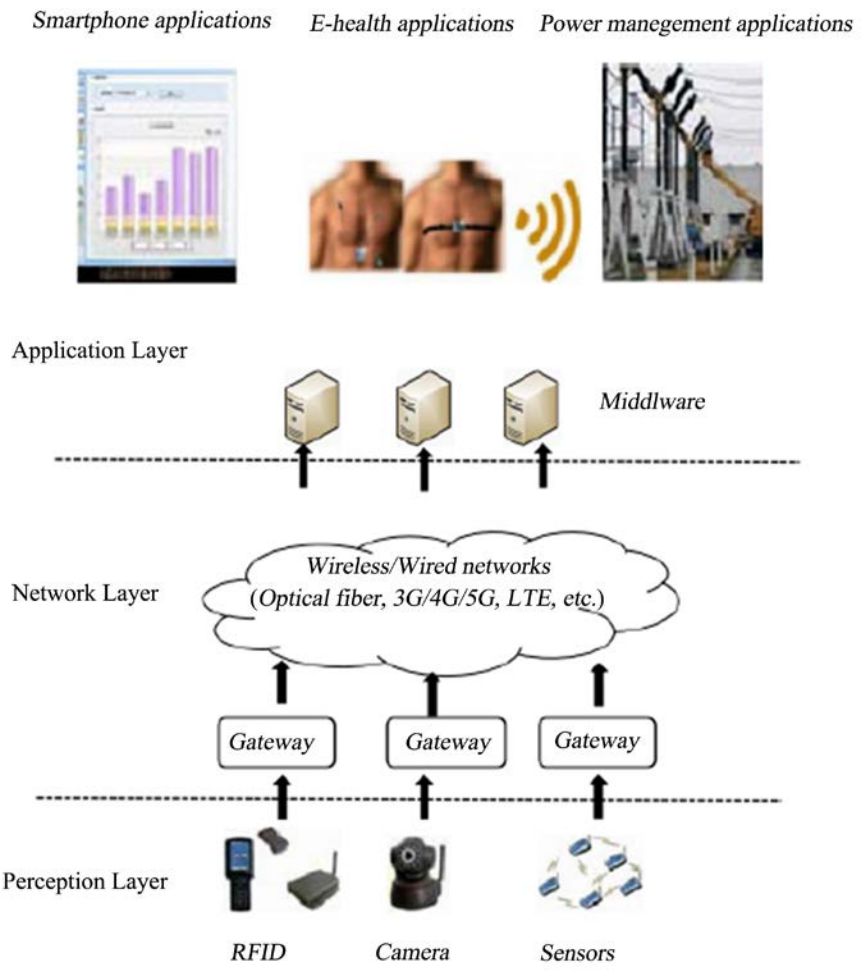

Figure 2. IoT architecture.

1) Description of the roles of the layers of the IoT architecture

- **The physical or perception layer**, also known as the sensing layer, which is the initial layer of the architecture, is where sensors and linked devices are used to collect various types of data as needed for the project. These might be the edge technology, computing hardware, object identification, and actuators that communicate with their surroundings and things addressing. Its goal is to perceive environmental data, as its name suggests. Frequency selection, modulation-demodulation, encryption-decryption, data transmission, and reception are a few further physical layer tasks. Energy usage, security, and interoperability are obstacles this layer must overcome [16].
- The **network layer**, the second tier in the architecture, is where the data gathered by each device needs to be transported to and processed. The MAC (Medium Access Control) in this **layer** forwards the data from sensing devices to the application layer for processing, analytics, and smart services. This layer links these gadgets to other smart items, servers, and network hardware. It also manages the data transmission for the entire system. Additionally, there are particular problems with the network layer regarding sca-

lability, network availability, power usage, and security [17].

- The user interacts with the **application layer**, also called the **services layer**, which is the third layer of the architecture. It is in charge of providing the user with services particular to that program. It offers clients smart services and also supplies the semantics layer with processed/aggregated data. Users may use this in their smart homes, for instance, by tapping a button in the app to start their coffee maker. The difficulties encountered at this layer involve managing, storing, and processing data obtained from the sensors, user information security and privacy, and compliance with industrial and governmental standards like those that safeguard users' rights to their health and personal information.
- **The sensing layer (smart processing layer)** is the fourth and last layer and is also known as a business management layer because it oversees all IoT system operations. The is layer collaborates closely with the application layer and uses intelligent computing approaches, including cloud computing, edge computing, and fog computing, to support the requirements of a variety of applications. It alludes to the use of cognitive technology in delivering a select number of high-end services, including data analysis, business intelligence, strategic decision-making, and business modeling.

Detailed in the diagram below in Figure 3 is IoT data flow from the server's edge.

2) Distinct Characteristics of IoT Smart Systems

a) Scalability and Interconnection

As a result of connectivity, any gadget can connect to the smart world, which ideally is essential in advancing smart city designs and is the most crucial component of a prosperous smart city [18]. Scalability is a noticeable characteristic in smart city scenarios. Scalable smart city systems and methods can function effectively despite the rapid expansion of smart cities from small to major cities, causing data and network traffic to grow at an accelerated rate.

b) Mobility

The emergence and development of contemporary cities have been credited in large part to urban mobility. Mobility in smart cities encompasses not just

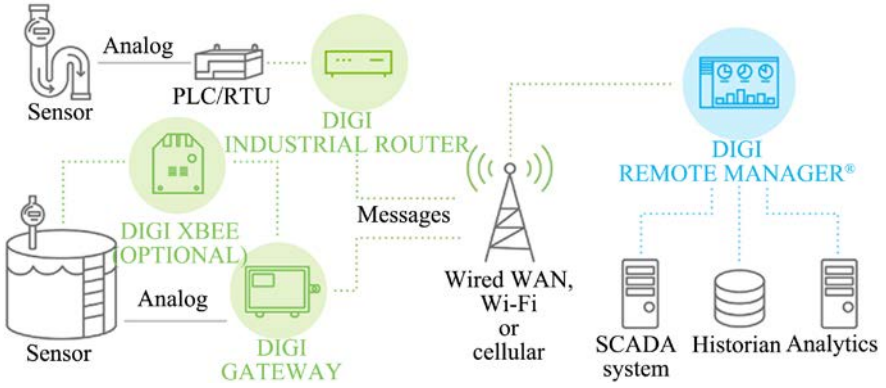

Figure 3. Data flow from the server/cloud.

movement within a city and the transportation of commodities to different locations, but also technology like citywide wireless connectivity, real-time traffic flow monitoring, and adaptable problem-solving techniques. The sophisticated communications infrastructure in smart cities also allows for personalized mobility.

c) Limited Resources

Due to low-power radio protocols, most IoT devices have restricted memory, battery life, and computing power in addition to restrictive network interfaces. More specifically, embedded devices that are less expensive and smaller but less energy-efficient frequently used in smart cities. These gadgets' storage and random-access memory capabilities are typically constrained, using 8-bit microcontrollers or 16-bit. According to [19], IEEE 802.15.4 radio-equipped wireless networks are to blame for the low data rates (20 - 250 kb/s and up to 127 octets) and short frame sizes (20 - 250 kb/s).

d) Heterogeneity

The most distinctive feature of IoT-based systems is their great heterogeneity, which refers to the fact that they are autonomous, distributed, and used or stored by various users. [20] defines heterogeneity as the large range of Internet of Things (IoT) nodes, communication protocols and technologies, mobility methods, various hardware performances, and platforms.

B. Smart Cities' Applications

IoT can be utilized in various ways to improve cities' efficiency since the central goal pod creation of smart cities is to help citizens in various ways that are directly relevant to their quality of life. The application areas include energy, environment, industry, lifestyle, and services with uses such as traffic management, air pollution control, waste management, designing more innovative structures, and disaster preparedness. **Figure 4** below highlights the new intelligent uses of smart cities and an in-depth about each one after that.

Numerous concerns, such as air pollution, a lack of fresh water, mountains of rubbish, and increased traffic, can develop when cities have population density problems. Both the public and private sectors have many potential applications for the Internet of Things. Smart cities can use IoT and smart technology in the following ways:

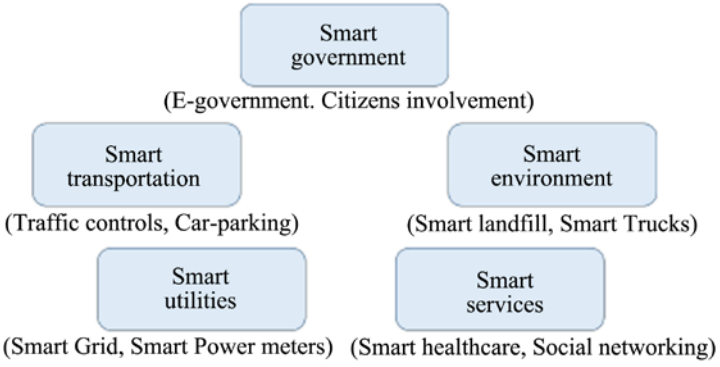

Figure 4. Smart cities' applications.

1) Air Quality Management

Smart cities are putting in place instruments to forecast emissions and gather pollution data in real-time. Accurate air pollution forecasting enables cities to identify the source of their emissions issues and develop tactical solutions to reduce the quantity of air pollution they emit. This will help build sustainable societies in an intelligent environment.

2) Smart Waste Management

Garbage management solutions aid in improving the effectiveness of waste collection, lowering operational costs, and more effectively resolving all environmental problems linked to ineffective waste collection. In these solutions, the waste container is equipped with a level sensor. When a predetermined threshold is reached, a truck driver's management platform notifies them via their smartphone. The message seems to empty a full container, assisting customers in avoiding drains with only half of their contents. This is helpful in environmental protection.

3) Smart Parking

Cities are utilizing automated parking technologies as well, which can detect when a car has left its spot. The driver can download a mobile app that uses sensors buried in the ground to notify the location of open parking spaces. Some people utilize vehicle responses to precisely locate openings and direct awaiting cars in the least difficult direction. This smart city application is perfect for a mid-sized smart city endeavor because smart parking is a reality now and does not require complex infrastructure or a significant investment.

4) Smart Solutions

Networking sites, entertainment, smart shopping, smart homes, and many other smarter service utilizations have made people's daily lives more convenient today. Citizens benefit from a variety of smart service features. By using wearable technology and medical sensors, for instance, intelligent healthcare applications can promptly monitor the health status of the patient who is using it [21]. Additionally, some smart services, like the ability to control home equipment from a distance, track items, home security systems, lost pets, and appliance maintenance appointments, are creating livable spaces that are smart, comfortable, and energy efficient (smart homes). Businesses can use IoT to track supply chains, follow customer spending patterns and feedback, maintain inventory levels, and do proactive maintenance on their machinery and devices. Customers can utilize the Internet of Things (IoT) to assist them in making restaurant reservations, keeping track of their fitness goals and general health, and receiving coupons for a store just by passing by the establishment in question.

5) Smart Utilities and Infrastructure

Cities' ability to support continual development is increasingly dependent on digital technologies. Cities are investing in electric and self-propelled vehicles to reduce CO_2 emissions. Intelligent technologies enable an infrastructure that is eco-friendlier and consumes less energy. To save energy, smart lighting, for instance, only illuminates when someone walks past it; other vital features of smart

lighting include the ability to control brightness and monitor daily usage. Smart cities need smart utilities to boost economic growth, safeguard the environment, and prevent overconsumption of resources like water and gas. Smart metering, a practical smart utility application, is widely used by smart grids to maintain track of dispersed energy supply [22].

6) Smart Government

A smart city needs a smart government since it aspires to better serve its citizens and communities by connecting information, institutions, operations, and infrastructure facilities using information technology [23]. It offers a practical means of streamlining and supporting improved planning and decision-making based on ICT tools. Connecting the relevant public, private, civil, and national institutions also helps an integrated smart city to emerge. Citizens can participate in public discussions and city planning thanks to smart governance [24], which can improve efficiency and information transparency. For instance, e-government allows citizens to access government services online, including paying bills, reporting difficulties, and applying for conference centers.

4. Threats to Security and Privacy Generated by the Development of Smart City IoT

Although above-mentioned advancements in smart cities have made a significant impact on society, nearly all smart applications are susceptible to hacking through contemporary attacks like background knowledge attacks, collusion attacks, Sybil attacks, eavesdropping attacks, spamming, inside curious attacks, outside forgery attacks, and identity attacks [25]. The possibility that systems are a target of cyberattacks has arisen due to the introduction of IoT, which connected City management systems to networks. According to reports from various studies, there is already a traffic of systems open to hacking. For instance, an assault on a smart city system might cause crucial urban functions to become unresponsive. Since the smart city manages data, including personal information, the best possible administration of such data is necessary. NEC has created a smart city function model based on documents released by the European Union Agency for Network Information Society and International Electro-Technical Commission to address the security requirements specific to the Smart City IoT. Listed below are some of the threats generated by the development of IoT Applications.

1) IoT-based Smart Cities' Botnet Activities

There is a growing risk of botnet attacks in IoT systems. IoT botnet malware is launched on a network connection of IoT devices, typically routers. Via a botnet DDoS attack, the users are denied access to the targeted servers or websites where several hacked systems work together to attack a single target. The attacker will create traffic to the device before disabling it.

2) Driverless car threats in smart cities

The rapid growth of AV use has been seen as a severe security threat since once an AV is compromised, life safety and data privacy are in danger [26].

Hackers can explicitly leverage security holes to launch remote attacks like slamming on the brakes, shutting off the engine, and adjusting the steering. The massive volumes of private data that a self-driving car's computer system collects in this scenario could raise significant privacy issues.

3) Virtual Reality Privacy Issues in Smart Cities

Storing sensor data and leveraging unencrypted connections between VR devices to transmit private information to third parties are all privacy leakage hazards [27]. Unfortunately, because they were rushed to market, these new programs' creators and users did not adequately and appropriately consider privacy.

4) Threats AI Poses to Smart Cities

It would seem that widespread AI use creates security flaws. Data mining technologies, for example, can be used by service providers and device makers to analyze personal data excessively and extract sensitive information that goes beyond the core objectives of the related services [28], but attackers who are knowledgeable about AI have become smarter [29].

Security Requirements for Safe and Secure Smart City IoT

A threat analysis method called STRIDE was used to sort out the threats and used the findings to identify the security requirements specific to the Smart City IoT, as will be discussed in this section.

1) Preventing data leaking and falsification

Even in contexts where a range of data kinds and various inter-service links exist simultaneously, it is necessary to avoid leaks and falsification since Smart City IoT systems manage both open and closed data. For instance, personal healthcare data is considered secure; tourist information is known as open data.

2) Prediction and Detection of Lightweight Intrusion

For a smart system to be considered secure, it should be able to monitor the circumstances au under which it operates and can quickly identify any unusual events due to the vulnerabilities of the devices and networks installed in a smart city. Most sensors and devices are resource-constrained; hence it is necessary to design lightweight intrusion detection techniques. Predicting risks and being aware of them beforehand is preferable to discovering them after an attack and trying to recover. According to Cui *et al.* [30], many intrusion prediction systems (IPS), particularly for web-based applications, frequently failed to identify and stop intrusions. Similarly, a study focusing on smart grids revealed that many hazardous intrusions are detected too late, making it impossible to take action after learning about the attack. Existing security control strategies are insufficient to secure a smart grid [31] adequately. It is crucial to design intelligent IPS systems to achieve security awareness and automatically foresee various attacks on smart apps.

3) Detecting and preventing device tampering

With Smart City IoT, devices are positioned all over the city streets to make them accessible to attackers. Determining altered or unauthorized devices as soon as possible is crucial, given that attackers could access a device directory and carry out data falsification or tampering. Furthermore, the entire system

must be robust, including IoT devices and the cloud. Because a Smart City IoT comprises IoT, gateways, servers, computers, and other devices, the attacker will target the system's weakest link, necessitating fine-tuning all the components to increase the system's overall robustness.

4) Authenticity and discretion

Throughout a heterogeneous system, authentication is a fundamental prerequisite to establishing identities and guarantees for various layers of a smart system [32]. The network, other nodes, and the communications from management stations can all be authenticated by IoT devices installed in smart cities. Due to the rapid expansion of the amount of authentication data n smart cities, it is crucial to create cutting-edge solutions to provide accurate and real-time authentication. Confidentiality/discretion is used to protect data from active or passive hacking attempts and unauthorized disclosure. Attackers are considered to be able to listen in on communications or access devices in IoT-based applications. Encryption-based technologies are frequently used to create reliable communication and storage systems, protecting the confidentiality of information transiting between nodes [33].

5) Integrity and accessibility

Intelligent programs or apps should be able to continue operating effectively even when under attack. A smart system must be able to recognize any abnormal conditions and be able to halt additional system damage because these devices are vulnerable to attacks. Smart Systems sough can withstand multiple defects and failures brought on by attacks and major disasters. Defense mechanisms must be strong and adaptive in their learning capabilities to counteract more intelligent attacks.

5. Modern Security and Privacy Protection Technologies for Smart Cities

- **Machine Learning (ML) and Data Mining**—Security infrastructures have frequently used ML technology to strengthen network defenses and counter threats. Secure data sensing, transmission, and ensuring privacy, machine learning-based methods have increasingly received attention. These methods were primarily proposed by Gavel *et al.* [34] for use in wireless sensor networks (WSNs), a vital component of the smart environment. Machine learning technologies to strengthen defense mechanisms in Smart cities' IoT and in making personalized decisions. The data mining technique is applied to search big data sets for anomalies, trends, and correlations to forecast results.
- **Cryptography**—Due to their ability to restrict access by untrustworthy parties during a data life cycle of storage, processing, and transmitting, cryptographic algorithms serve as the foundation for security and confidentiality control for the operations of smart cities' systems and applications [35]. Cryptographic algorithms have therefore been the standard technology for effective security controls. Zero-knowledge proofs, homomorphic encryption, and lightweight authentication techniques are a few examples.

- **Game Theory**—A potent mathematical tool known as game theory has been effectively used in several applications, including cybersecurity and privacy protection [36] [37]. Most research that addresses privacy-related concerns creates mechanisms by integrating game theory with other privacy-protection techniques [38] [39]. In cybersecurity, game theory can examine the dynamics of a cyber event, where users, attackers, and network defenses interact to achieve a result. Game theory is a helpful tool to balance data utility with protection intensity, as demonstrated by the strategy put forth by Balamurugan & Biswas [40] in 2015. However, the game of theory mechanism has been employed in very few IoT applications.
- **Biometrics**—Biometrics technology is frequently used in IoT-based systems for authentication, particularly to instantly identify a person based on distinctive behavioral and biological traits. Fingerprints, faces, voices, handwritten signatures, and other biometric data are used to retrieve the information. Brainwave-based authentication [41] is one technique that merits attention in this context since it can guarantee efficiency while also achieving a high level of authentication accuracy. Chen *et al.* [42] presented a key negotiation and mutual authentication system to safeguard users' private data stored on storage devices. In addition to successfully thwarting security assaults, the unique protocol also maintains a reasonable communication cost and overhead compared to previous analogous systems. However, inappropriate use of these bio-based systems increases the risk of privacy leakage

Challenges faced and Potential opportunities for future studies

New, efficient solutions are required to address the most recent issues in this type of complicated environment. IoT applications for building smart cities appear to be few and far between. Over 70% of the world's people live in cities [43] and could benefit from digital cities in the future if safe and secure requirements are considered. Building smart cities are still challenging, even though many of these applications are now used in significant urban areas worldwide. Some of these reasons include bureaucracy or the time it takes to integrate new technology with existing systems.

1) Lightweight Security Solutions

Despite the recent development of numerous security and privacy mechanisms, using some of these processes is impracticable in IoT. Due to sensors and device's low processing power and energy sources, simple and weakly preserving algorithms should be used. Therefore, further research studies are required to develop a lightweight security mechanism to ensure protection, flexibility, and dynamic and low-cost requirements [44].

2) Issues with security and privacy in fog-based systems

Fog-based systems, a technology springing up in smart city implementation, pose new security difficulties because the environments in which they operate are more open to intrusions than centralized clouds are. Fogs have smaller defense systems than clouds, which limits their capacity for self-defense. Additionally, because Fog nodes are situated near end users, they present priceless

chances to safeguard customer privacy before their private information leaves the edge. Therefore, there should be more focus on intelligent device protections in Fog-based smart systems [45].

3) Smart cities' IoT-based network security

IoT is a network of networks that connects and integrates heterogeneous networks, including the Internet, mobile networks, social networks, and industrial networks [46]. In such a complicated environment, new, efficient solutions required to meet the most recent issues [47]. For instance, modeling the dissemination of information patterns in WSN, understanding the features of malware transmission in IoT-based infrastructures, and developing effective protection techniques are all very important [48].

4) Using Blockchain to Improve Security of IoT Systems

A blockchain is a decentralized peer-to-peer network that stores a registry of unchangeable transactions. Some of the significant security and privacy advantages of Blockchain, including decentralized authentication, the integrity of the transaction, and built-in defense against ransomware and crypt locker-style assaults, can be used in the IoT. However, further investigation and research are needed to implement it in IoT devices [49].

5) The integrity of the Program/Code

There are many ways to guarantee the integrity of IoT end devices. However, the most reliable ones necessitate executing the entire attestation process in a secure setting. However, creating secure hardware-based IoT solutions for uses other than the essential infrastructure is unrealistic due to the deployment size and cheap cost of IoT devices. Therefore, it is necessary to have safe solutions based on software that can be developed quickly with few resources and are adaptable for timely upgrades. The Internet of Things will consist of many heterogeneous devices in the future. Therefore, creating a mechanism that will effectively alert, identify and repair any malicious software modifications is difficult [50].

6. Summary and Conclusion

These days, the communication protocols' built-in security does not defend against malware and attacks due to node compromise. Additionally, given the current spike in the number of ransomware attacks, the primary cause of the negative impacts of the development of smart systems has been attributed to centralized network architecture, where all the functionalities of networking and security activities are handled centrally. On the other side, such centralized network architectures are expensive to set up, presenting single points of failure. Blockchain technology is being investigated and tested due to its unforgeable distributed design to address the security and privacy challenges of IoT, among other approaches. Due to the ability of the Blockchain to run distributed programs in the form of smart contracts and store data on various nodes, Blockchain is thought to be able to address the majority of the data integrity challenges associated with the Internet of Things.

The majority of known dangers to IoT systems, ranging from essential message interception to complex malware attacks, have been attempted to be highlighted in this paper. Additionally, a comprehensive set of security guidelines based on industry best practices have been provided in this article, which can assist IoT standardization bodies in creating minimal security requirements depending on the different categories of IoT applications and devices. Research issues around IoT security have been explored to help people better comprehend the threat spectrum. The numerous security needs of these quickly evolving innovative applications demand a lot to be satisfied. Creating more sophisticated protection frameworks and models is crucial and in great demand in both the academic and industrial worlds. It is safe to expect that the focus of studies on smart cities in the coming years will be on addressing the problems that have been identified.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Yahia, N.B., Eljaoued, W., Saoud, N.B.B. and Colomo-Palacios, R. (2021) Towards Sustainable Collaborative Networks for Smart Cities Co-Governance. *International Journal of Information Management*, **56**, Article ID: 102037. https://doi.org/10.1016/j.ijinfomgt.2019.11.005

[2] Yu, W. and Xu, C. (2018) Developing Smart Cities in China: An Empirical Analysis. *International Journal of Public Administration in the Digital Age* (*IJPADA*), **5**, 76-91. https://doi.org/10.4018/IJPADA.2018070106

[3] Manfreda, A., Ljubi, K. and Groznik, A. (2021) Autonomous Vehicles in the Smart City Era: An Empirical Study of Adoption Factors Important for Millennials. *International Journal of Information Management*, **58**, Article ID: 102050. https://doi.org/10.1016/j.ijinfomgt.2019.102050

[4] Yeh, H. (2017) The Effects of Successful ICT-Based Smart City Services: From Citizens' Perspectives. *Government Information Quarterly*, **34**, 556-565. https://doi.org/10.1016/j.giq.2017.05.001

[5] Cividino, S., Halbac-Cotoara-Zamfir, R. and Salvati, L. (2020) Revisiting the "City Life Cycle": Global Urbanization and Implications for Regional Development. *Sustainability*, **12**, Article 1151. https://doi.org/10.3390/su12031151

[6] Sabou, G.C. and Maiorescu, I. (2020) Cybersecurity Challenges in Smart Cities—A Smart Governance Perspective. *IBANESS Congress Series on Economics*, *Business and Management*, Plovdiv, Bulgaria, 26-27 September 2020, 167-171.

[7] Ismagiloiva, E., Hughes, L., Rana, N. and Dwivedi, Y. (2019) Role of Smart Cities in Creating Sustainable Cities and Communities: A Systematic Literature Review. In: Dwivedi, Y., Ayaburi, E., Boateng, R. and Effah, J., Eds., *International Working Conference on Transfer and Diffusion of IT*, Springer, Cham, 311-324. https://doi.org/10.1007/978-3-030-20671-0_21

[8] Barreto, C., Neema, H. and Koutsoukos, X. (2020) Attacking Electricity Markets through IoT Devices. *Computer*, **53**, 55-62.

https://doi.org/10.1109/MC.2020.2973951

[9] Wazid, M., Das, A.K., Odelu, V., Kumar, N. and Susilo, W. (2017) Secure Remote User-Authenticated Key Establishment Protocol for Smart Home Environment. *IEEE Transactions on Dependable and Secure Computing*, **17**, 391-406. https://doi.org/10.1109/TDSC.2017.2764083

[10] Sokak, M., Tang, H., He, Y. and Yu, F.R. (2018) Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, **21**, 1718-1743. https://doi.org/10.1109/COMST.2018.2867288

[11] Bagga, P., Das, A.K., Wazid, M., Rodrigues, J.J., Choo, K.K.R. and Park, Y. (2021) On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. *IEEE Transactions on Vehicular Technology*, **70**, 1736-1751. https://doi.org/10.1109/TVT.2021.3050614

[12] Davis, B.D., Mason, J.C. and Anwar, M. (2020) Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal*, **7**, 10102-10110. https://doi.org/10.1109/JIOT.2020.2983983

[13] Görmüş, S., Aydın, H. and Ulutaş, G. (2018) Security for the Internet of Things: A Survey of Existing Mechanisms, Protocols and Open Research Issues. *Journal of the Faculty of Engineering and Architecture of Gazi University*, **33**, 1247-1272.

[14] Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.A. and Hong, C.S. (2019) Internet of Things Forensics: Recent Advances, Taxonomy, Requirements, and Open Challenges. *Future Generation Computer Systems*, **92**, 265-275. https://doi.org/10.1016/j.future.2018.09.058

[15] Angrishi, K. (2017) Turning Internet of Things(IoT) into Internet of Vulnerabilities (IOV): IOT Botnets. https://arxiv.org/abs/1702.03681

[16] Jasim, N.A. and Alrikabi, H.T.S. (2021) Design and Implementation of Smart City Applications Based on the Internet of Things. *International Journal of Interactive Mobile Technologies*, **15**, 4-15. https://doi.org/10.3991/ijim.v15i13.22331

[17] Anand, R., Sindhwani, N. and Juneja, S. (2022) Cognitive Internet of Things, Its Applications, and Its Challenges: A Survey. In: Bala, I. and Ahuja, K., Eds., *Harnessing the Internet of Things* (*IoT*) *for a Hyper-Connected Smart World*, Apple Academic Press, 91-113. https://doi.org/10.1201/9781003277347-5

[18] Khanna, A. and Kaur, S. (2020) Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wireless Personal Communications*, **114**, 1687-1762. https://doi.org/10.1007/s11277-020-07446-4

[19] Betancur, V.T. (2018) Management of Resource-Constrained IoT Devices in Urban Scenarios. Science: Internet, Data and Things (CS-E4000), Spring 2018, 55.

[20] Kaur, S. and Kaur, G. (2022) Internet of Things (IoT): Issues and Challenges Ahead. *Journal of Business Management*, **1**, 1-4. https://doi.org/10.56388/bm220712

[21] Oliveira, E., da Rocha, A.R., Mattoso, M. and Delicato, F.C. (2022) Latency and Energy-Awareness in Data Stream Processing for Edge Based IoT Systems. *Journal of Grid Computing*, **20**, Article No. 27. https://doi.org/10.1007/s10723-022-09611-4

[22] Raza, N., Akbar, M.Q., Soofi, A.A. and Akbar, S. (2019) Study of Smart Grid Communication Network Architectures and Technologies. *Journal of Computer and Communications*, **7**, 19-29. https://doi.org/10.4236/jcc.2019.73003

[23] Sasha, I. and Gil-Garcia, J.R. (2019) A Collaborative Governance Approach to Partnerships Addressing Public Problems with Private Data. *Proceedings of the* 52*nd Hawaii International Conference on System Sciences*, Hawaii, 8-11 January 2019. 1-10. https://doi.org/10.24251/HICSS.2019.350

[24] Jiang, H., Geertman, S. and Witte, P. (2020) Avoiding the Planning Support System Pitfalls? What Smart Governance Can Learn from the Planning Support System Implementation Gap. *Environment and Planning B*: *Urban Analytics and City Science*, **47**, 1343-1360. https://doi.org/10.1177/2399808320934824

[25] Antoniadis, I.I., Chatzidimitriou, K.C. and Symeonidis, A.L. (2019) Security and Privacy for Smart Meters: A Data-Driven Mapping Study. 2019 *IEEE PES Innovative Smart Grid Technologies Europe* (*ISGT-Europe*), Bucharest, Romania, 29 September 2019-2 October 2019, 1-5. https://doi.org/10.1109/ISGTEurope.2019.8905611

[26] Elkhwesky, Z. and Elkhwesky, E.F.Y. (2022) A Systematic and Critical Review of Internet of Things in Contemporary Hospitality: A Roadmap and Avenues for Future Research. *International Journal of Contemporary Hospitality Management*. https://doi.org/10.1108/IJCHM-01-2022-0090

[27] Bastug, E., Bennis, M., Médard, M. and Debbah, M. (2017) Toward Interconnected Virtual Reality: Opportunities, Challenges, and Enablers. *IEEE Communications Magazine*, **55**, 110-117. https://doi.org/10.1109/MCOM.2017.1601089

[28] Khanna, A. and Kaur, S. (2020) Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wireless Personal Communications*, **114**, 1687-1762. https://doi.org/10.1007/s11277-020-07446-4

[29] Acquisti, A., Brandimarte, L. and Loewenstein, G. (2020) Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, **30**, 736-758. https://doi.org/10.1002/jcpy.1191

[30] Cui, L., Xie, G., Qu, Y., Gao, L. and Yang, Y. (2018) Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access*, **6**, 46134-46145. https://doi.org/10.1109/ACCESS.2018.2853985

[31] Mishra, S. and Dehury, N. (2021) Big Data Analytics for Smart Grids, the Cyber-physical System in Energy—A Bibliographic Review. In: Das, S. and Mohanty, M.N., Eds., *Advances in Intelligent Computing and Communication*, *Lecture Notes in Networks and Systems*, Springer, Singapore, 437-447. https://doi.org/10.1007/978-981-16-0695-3_42

[32] Soni, M. and Singh, D.K. (2021) LAKA: Lightweight Authentication and Key Agreement Protocol for Internet of Things Based Wireless Body Area Network. *Wireless Personal Communications*, **127**, 1067-1084. https://doi.org/10.1007/s11277-021-08565-2

[33] Fredriksson, A., Sezer, A.A., Angelakis, V. and Gundlegård, D. (2022) Construction Related Urban Disturbances: Identification and Linking with an IoT-Model. *Automation in Construction*, **134**, Article ID: 104038. https://doi.org/10.1016/j.autcon.2021.104038

[34] Gavel, S., Charitha, R., Biswas, P. and Raghuvanshi, A.S. (2021) A Data Fusion Based Data Aggregation and Sensing Technique for Fault Detection in Wireless Sensor Networks. *Computing*, **103**, 2597-2618. https://doi.org/10.1007/s00607-021-01011-y

[35] Kaur, S. and Kaur, G. (2022) Internet of Things (IoT): Issues and Challenges Ahead. *Journal of Business Management*, **1**, 1-4. https://doi.org/10.56388/bm220712

[36] Do, C.T., Tran, N.H., Hong, C., Kamhoua, C.A., Kwiat, K.A., Blasch, E., Iyengar, S.S., *et al.* (2018) Game Theory for Cyber Security and Privacy. *ACM Computing Surveys* (*CSUR*), **50**, 1-37. https://doi.org/10.1145/3057268

[37] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R.P. and Ni, W. (2018) Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys & Tutorials*, **21**,

1636-1675. https://doi.org/10.1109/COMST.2018.2874978

[38] Xu, X., Chen, H. and Xie, L. (2021) A Location Privacy Preservation Method Based on Dummy Locations in Internet of Vehicles. *Applied Sciences*, **11**, Article 4594. https://doi.org/10.3390/app11104594

[39] Gilliam, G. and Uhan, N.A. (2022) Computing Payoff Allocations in the Approximate Core of Linear Programming Games in a Privacy-Preserving Manner. *Operations Research Letters*, **50**, 64-71. https://doi.org/10.1016/j.orl.2021.12.008

[40] Balamurugan, B. and Biswas, D. (2018) Security in Network Layer of IoT: Possible Measures to Preclude. Security Breaches and Threat Prevention in the Internet of Things, IGI Global, 46-75. https://doi.org/10.4018/978-1-5225-2296-6.ch003

[41] Hwang, S.-H. and Liu, S.-Z. (2019) Survey on 3GPP Low Power Wide Area Technologies and Its Application. 2019 *IEEE VTS Asia Pacific Wireless Communications Symposium* (*APWCS*), Singapore, 28-30 August 2019, 1-5. https://doi.org/10.1109/VTS-APWCS.2019.8851631

[42] Chen, M., Miao, Y., Jian, X., Wang, X. and Humar, I. (2018) Cognitive-LPWAN: Towards Intelligent Wireless Services in Hybrid Low Power Wide Area Networks. *IEEE Transactions on Green Communications and Networking*, **3**, 409-417. https://doi.org/10.1109/TGCN.2018.2873783

[43] Cividino, S., Halbac-Cotoara-Zamfir, R. and Salvati, L. (2020) Revisiting the "City Life Cycle": Global Urbanization and Implications for Regional Development. *Sustainability*, **12**, Article 1151. https://doi.org/10.3390/su12031151

[44] Yassine, H. and Malli, M. (2019) A Lightweight IoT Security Solution. 2019 15*th International Wireless Communications & Mobile Computing Conference* (*IWCMC*), Tangier, Morocco, 24-28 June 2019, 567-572. https://doi.org/10.1109/IWCMC.2019.8766687

[45] Nooribakhsh, M. and Mollamotalebi, M. (2020) A Review on Statistical Approaches for Anomaly Detection in DDoS Attacks. *Information Security Journal*: *A Global Perspective*, **29**, 118-133. https://doi.org/10.1080/19393555.2020.1717019

[46] Qi, Q. and Tao, F. (2019) A Smart Manufacturing Service System Based on Edge Computing, Fog Computing, and Cloud Computing. *IEEE Access*, **7**, 86769-86777. https://doi.org/10.1109/ACCESS.2019.2923610

[47] He, S., He, P., Chen, Z., Yang, T., Su, Y. and Lyu, M.R. (2021) A Survey on Automated Log Analysis for Reliability Engineering. *ACM Computing Surveys* (*CSUR*), **54**, 1-37. https://doi.org/10.1145/3460345

[48] Aldhaheri, S. and Almagwashi, H. (2019) A Comparative Research between the KSA and UAE Cybercrimes Legislations. *International Journal of Computer Science and Information Security* (*IJCSIS*), **17**, 62-66.

[49] Nofer, M., Gomber, P., Hinz, O. and Schiereck, D. (2017) Blockchain. *Business & Information Systems Engineering*, **59**, 183-187. https://doi.org/10.1007/s12599-017-0467-3

[50] Ankergård, S.F.J.J., Dushku, E. and Dragoni, N. (2021) State-of-the-Art Software-Based Remote Attestation: Opportunities and Open Issues for Internet of Things. *Sensors*, **21**, Article 1598. https://doi.org/10.3390/s21051598