International Journal of Decision Inelligence
Vol 1, Issue 4, Autumn 2024, 23-33

Data Security and Privacy Challenges in IoT-Enabled Smart Cities: A Comprehensive Survey

Safoura Akhlaghi[a,]*, Mohammad Bagher Menhaj[b], Behrooz Masoumi[c]

[a]Department of Computer Engineering and Information Technology Islamic Azad University of Qazvin, Qazvin, Iran
[b]Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran
[c]Department of Computer Engineering and Information Technology Islamic Azad University of Qazvin, Qazvin, Iran

Received 15 September 2024; Accepted 22 October 2024

Abstract

The rapid expansion of IoT technology has given rise to smart cities, but their complex architecture poses security challenges at various levels. Security and privacy are paramount requirements in the development of smart cities, particularly with the proliferation of IoT devices and data-driven systems.Since the privacy and security of smart city data in the IoT is a very up-to-date topic, researchers have addressed this issue, and several review articles have been conducted in this field. Addressing the intricate challenges posed by these advancements is crucial to safeguarding sensitive information against evolving attack vectors. This paper introduces a systematic literature review method to investigate privacy and security in IoT-based smart cities, analyzing research from 2016-2024. We present a taxonomy based on smart city architecture, categorizing privacy and security into low, middle, and high levels. This study reviews and categorizes articles, discusses their findings, methods, benefits, and drawbacks, and highlights future research areas in smart city security and privacy.

Keywords: Smart city, Internet of Things, Security, Privacy, Fog computing, Artificial intelligence

I. INTRODUCTION

The concept of IoT was expressed in 1999 to develop the concept of Radio Frequency Identification (RFID) by Kevin Ashton [1]. Widespread use of the IoT made it very popular in 2010, and the Chinese government launched a five-year IoT program that made the IoT more popular. IoT is a system of equipment, sensors, hardware, and physical devices that connect to the Internet and can receive and monitor various data from devices [3]. IoT is a new idea and technology that has greatly affected human life and made it more accessible and smarter for people to live and work. The astonishing effects of the Internet of Things are not limited to their home life but also profoundly affect business and industry. One of the most fundamental effects of using IoT technology in industrial production is that things are done automatically and reduces the costs of human resources, manufacturing, and shipping products, as well as many other positive effects. The positive impact of using the Internet of Things can be seen in transportation, communications, industry, trade, environment, medicine, education, home security, children's toys, and much more [2]. By 2020, approximately 34 million IoT devices will be used worldwide [4]. More people have recently settled in cities, and the UN estimates that by 2050, About two-thirds of the world's people, about 68 percent, will live in cities. In recent years, the popularity and importance of smart cities have increased dramatically. As the evidence shows, the next generation will be urban. Despite the large population living in cities, it is essential to provide a comfortable life in which urban living conditions, food, resource needs, etc., are met. Fortunately, the IoT helps make this possible and makes it possible. Many cities are trying to increase the quality and comfort of people living in these cities by becoming smart cities. Paris and London are among the smart cities with high intelligence levels [5]. China has also focused on more than 200 projects to achieve smart cities [6]. Many researchers, both in industry and academia, have addressed and will continue to address the issue of smart cities. The smart city is a city where technologies, equipment, and resources have been used intelligently and aim to improve the quality and comfort of urban life [7]. Smart health care, smart building, smart economy, smart energy consumption, smart transportation, intelligent traffic control, and much more are among the most important applications of smart cities.

Indeed, one of the most important and main initiatives of the smart city is IoT technology, this powerful technology that has enabled the digitalization of learners and created the concept of smart cities. In the IoT platform, all equipment is connected to the Internet. They are allowed to send information through the cloud platform and receive information through specific and potential routes. IoT includes data collection and data collection and implementation of data analysis and analysis operations to extract useful information to support appropriate decision-making and overall policy making. People working in the field have estimated that by the end of 2025, about 75 billion devices and equipment will be connected to the Internet [8], leading to more applications' development. In smart city infrastructure, IoT allows sensors in the system to collect and send city status data to a central cloud. The targets and patterns intended for the smart city are extracted and used using this collected data. One of the most important and necessary issues in using IoT in smart cities is the issue of privacy and data security. Security generally means a person's right not to be supervised by others [9]. It is clear that the security issue in smart cities goes far beyond surveillance and non-harassment, and the security of personal data must be protected in many respects. For example, security related to each person's physical location, identity information, bank account information and personal passwords, information about a person's thoughts and feelings, and the habits of many others should be maintained. For example, in smart medicine, patients' information about the disease and name must be sufficiently secure.

Another example is in smart homes, information about the presence of people in their own homes and the home password must be confidential [10]. For example, when we talk about security in smart vehicles, there is information about passengers, such as their name and destination, information about the owners of smart vehicles, the current location of the vehicle, and much more about it [10]. For example, keeping account and password information when shopping online and the recipient's address information to receive the package is very important [11]. These are just a few examples of the importance of protecting the privacy and security of your data. Currently, there are numerous applications and benefits of the Internet of Things.

On the other hand, there are multiple concerns, the most important of which is the issue of data privacy and security, as the security and privacy of smart city data in Internet Objects can be compromised. For example, the security of a person's physical location can be threatened by the Global Positioning System (GPS) or other systems equipped with location, or information about a person's feelings and beliefs, such as religion and politics, can be disclosed through smartphones and social networks. Another is the information about individuals' bank accounts and addresses, which can be disclosed online shopping. Many other things can lead to the destruction and threat to the privacy and security of personal data. Therefore, it is essential to address the security issue specifically and precisely.

Unfortunately, today, due to the large volume of data and various information collected through different technologies and tools of the devices and then processed and stored, maintaining security and privacy has not been an easy task and has many difficulties. Given the importance of security, it must be taken seriously. In other words, data is the core and most important part of a smart city that contains information about users and should be well cared for and maintained. For example, GPS can reveal information about users' physical location if they are not secure enough. Security is related to various fields, such as personal habits, personal identity information, information about physical location, etc. [9].

Since the privacy and security of smart city data in the IoT is a very up-to-date topic, researchers have addressed this issue, and several review articles have been conducted in this field. Review paper [6] Examine key privacy and security issues in smart city application architecture and some solutions. Paper [7] has thoroughly addressed smart cities' security and privacy issues. They also reviewed the measures taken in this regard and examined their strengths and weaknesses. Paper [9] examined the state of smart cities worldwide and discussed how individuals' privacy was compromised and how data was protected. The most crucial goal of this article is to examine the issue of security and privacy in smart cities to provide concepts, original texts, architectures, and various tools in this field. In this article, we will review the work and studies that have already been done in the field of security and privacy in smart cities and talk about various issues, problems, tools, challenges, and other issues in this field.

The paper's key contributions are as follows:

- Introduction of a detailed technical taxonomy for categorizing IoT-based smart city security and privacy topics.
- Identification of future research challenges, specific issues, and overall challenges in the field.
- Discussion of primary challenges within smart city security and privacy.

The subsequent sections will be structured as follows: Section II reviews related work and previous research. Section III outlines the research methodology and motivations for using the Systematic Literature Review (SLR) model. Section IV offers a systematic description and classification of extensive research studies on security and privacy in smart cities. Section V presents a comprehensive analysis, addressing research questions, open topics, and future trends. Section VI concludes the paper, highlighting its limitations.

All abbreviations used in this article are listed in Table I to avoid ambiguity and confusion.

TABLE I. LIST OF ABBREVIATIONS

Abbreviation	Full name
SLR	Systematic Literature Review
DSM	Data Management System
GAN	Generative Adversarial Networks
RFID	Radio Frequency Identification
PETs	Privacy-Enhancing Technologies
TCNN	Temporal Convolution Neural Network

GPS	Global Positioning System
ML	Machine Learning
IDS	Intrusion Detection System
DL	Deep Learning
EMR	Electronic Medical Records
AI	Artificial Intelligence
RQ	Research Question
IoT	Internet of Things

II. Related work

A systematic review of privacy identifiers in IoT environments and aliasing methods is done in [6]. Categorized aliasing approaches and discussed IoT environments. This paper introduced a new pseudonym classification but focused on a privacy-enhancing method and limited its comprehensiveness. In [7], privacy in IoT systems based on cloud and edge computing is investigated. It covers data, location, and identity privacy and categorizes open research topics into different aspects of the system. However, it mainly focused on two architectural scenarios in IoT and ignored the diversity of complex systems. Privacy protection in smart vehicles in smart cities and approaches, technologies, classifications, and solutions are covered in [8]. It categorized privacy solutions into data-driven and process-driven. Still, the scope of PET technologies was limited, and broader privacy and security issues in smart city and vehicle communications were ignored. In [9], smart city implementations worldwide are reviewed, and privacy practices and enhancement technologies are discussed. However, it did not evaluate performance metrics for privacy-enhancing technologies or operationalize smart city device solutions. Ethical, privacy, and security challenges in the IoT, along with related laws and emerging standards, are reviewed in [10]. In [11], the authors analyzed data integration in smart cities and proposed a multi-point data classification. They discussed data integration techniques but limited their focus to the application level, omitting an in-depth analysis of domain-specific requirements and techniques. A comprehensive review of privacy-preserving mechanisms in crowd sensing systems, where data are collected from large groups of users via sensors or mobile devices, is presented in [12]. The authors discuss existing techniques for protecting user privacy and examine the challenges associated with protecting sensitive information while maintaining data quality and utility. Key research challenges identified include finding a balance between privacy, accuracy, and scalability with increasing data volumes in IoT and crowd sensing applications. In [13], it discusses privacy-preserving techniques for IoT and proposes an outline architecture for privacy assurance. The authors review existing privacy-preserving solutions and suggest ways to efficiently implement these techniques in large-scale IoT systems. Their design architecture aims to provide a comprehensive approach to address privacy issues, focusing on scalability and real-world applicability while addressing data security, user control, and privacy risks in IoT environments. In another similar work [14], existing privacy protection approaches for IoT environments are reviewed. It provides an overview of current methods and categorizes them according to their performance and effectiveness. This paper highlights various challenges facing IoT privacy, such as the heterogeneity of IoT devices, resource limitations, and the growing scale of IoT networks. The authors call for further research to develop robust, scalable, and efficient privacy mechanisms to protect user data in the evolving IoT landscape.

The literature review summarizes the most recent research in Table II, highlighting key studies and their limitations. The identified weaknesses in existing studies include:

- One-Dimensional Approach: Many review articles in Table II examine only one aspect of IoT and smart cities, neglecting comprehensive evaluations of solutions and challenges.
- Lack of Precise Issue Classification: A one-dimensional approach hinders precise issue classification, making it challenging to navigate the research landscape effectively.
- Need for Up-to-date Comprehensive Studies: Given the rapidly evolving IoT and smart city field, up-to-date and comprehensive studies using systematic research are essential to address the ever-expanding challenges in this area.

TABLE II. Overview of Studies on Privacy and Security in Smart Cities

Ref.	Topic	Publisher	Year	Citation
[6]	Privacy-preserving identifiers for IoT	IEEE	2020	6
[7]	Privacy-preserving in Industrial IoT	IEEE	2020	9
[8]	PETs are applied to connected vehicles within smart city environments.	WILEY	2020	2
[9]	PETs for smart cities	ELSEVIER	2019	41
[10]	Security, Ethics, Privacy, and Laws challenges in IoT	ELSEVIER	2021	14
[11]	Data in Smart City applications	ELSEVIER	2019	127
[12]	Privacy-preserving mechanisms for crowdsensing	IEEE	2016	100
[13]	Privacy-preserving IoT environments	ELSEVIER	2017	155
[14]	Privacy-preserving IoT environments	WILEY	2018	117

III. Methodology

Here, we offer an in-depth explanation of the research process followed in this Systematic Literature Review (SLR). More specifically, this section includes three main sections under the headings "research purpose and questions," "research resources and strategy," and " inclusion-exclusion criteria and articles selection."

A. Purposed research questions

This review article aims to conduct an unbiased SLR to comprehensively examine and categorize key questions in the field, providing an overview of the relevant literature. Our main objective is to thoroughly address privacy and security challenges in smart cities within the IoT. We aim to explore existing studies covering issues associated with this rapidly expanding technology. Additionally, we intend to assess proposed solutions, including models and architectures, to determine their effectiveness and practicality in mitigating these challenges. We structured the review by defining the research questions (RQs) as follows:

- **RQ1.** What are the most important smart city privacy challenges in the IoT environment?
- **RQ2.** What techniques have been used to solve IoT privacy issues, and how can they be implemented?
- **RQ3.** What metrics are essential and can be taken to measure privacy and security in smart cities?
- **RQ4.** What are smart cities' challenges, issues, open topics, and future orientations in the IoT context?

We aim to address these questions through this SLR, leveraging previous research to inform future studies and enhance privacy methods, tools, and regulations for smart cities. The insights from this study will contribute to the safe implementation of smart cities in practice. Additionally, in the final stages of this research, we will explore emerging trends and open challenges in securing smart cities within the IoT context.

B. Research resources and strategies

We developed our search strategy using chosen keywords and mathematical operators based on the outlined research questions (RQs). To ensure comprehensive coverage of research relevant to each question, we formulated specific search fields as follows:

- Privacy preservation, security, IoT, challenges, smart city, and IoT.
- Tools for implementing privacy preservation.
- Techniques for addressing IoT privacy preservation issues.

We searched various search engines using these fields and identified pertinent articles across well-known publishers, including IEEE, Springer, ELSEVIER, Wiley, and MDPI.

C. Inclusion-Exclusion criteria and articles selection

We started with the initial list and then looked at specific criteria for obtaining articles that were more focused on the review based on these criteria. More specifically, we considered a set of inclusion and exclusion criteria in reviewing our selected articles, which can be seen in Table 3. For example, one of our inclusion criteria was articles written in English. Also, articles written before 2016 were removed to continue the research. Based on these criteria in Table III, we could identify articles for this review and store them in the initial list of selected articles. Then we read the existing articles, deleted the irrelevant articles, put the approved articles in the final list of selected articles, and used them for analysis. The exact steps used in this methodology are fully summarized in Figure 1.

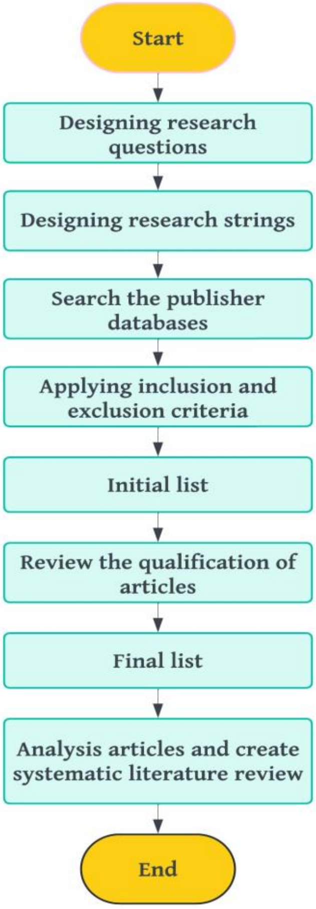
Start
Designing research questions
Designing research strings
Search the publisher databases
Applying inclusion and exclusion criteria
Initial list
Review the qualification of articles
Final list
Analysis articles and create systematic literature review
End

Fig. 1. A summary of the methodology used.

TABLE III. INCLUSION-EXCLUSION CRITERIA USED IN THE RESEARCH.

Inclusion criteria
• Articles with higher citations and newer publication year • Articles related to privacy-preserving techniques in smart cities • Articles which are proposed methods for privacy preserving in smart cities • Articles that are written in the English language only
Exclusion criteria
• Articles that had less to do with privacy • Articles published in low-level journals • Articles related to the years before 2016 • Articles published in black-listed journals

IV. Background of the Privacy and Security of Smart Cities in IoT

This section provides an in-depth overview of privacy and security issues in smart cities, emphasizing the IoT. Our organization categorizes security and privacy into three main categories: low, medium, and high layers. In our proposed architecture, we merge the two middleware layers and the Network layer into the middle layer, comprising two sub-sections: privacy and security in data and communications. The Application and Business layers are considered part of the cloud layer. Subsequent sections of the article provide a detailed examination of this categorization.

A. Security threats in low-level infrastructure

Today, several billion IoT devices are deeply located in the physical world. These devices receive helpful and valuable data and understand that it enables many of the smart apps created to be built and produced based on them. As a result, they have made the most critical decisions to control and challenge the physical world and smart cities. Here, we explore IoT security frameworks in smart cities, particularly focusing on edge-level devices researched over the past few years. The authors in [15] improved mobile device security and performance in crowdsensing systems. They proposed an efficient and private fact discovery and privacy plan (EPTD) for congestion measurement, using data aggregation with privacy-preserving techniques. The security evaluation ensured confidentiality and strong privacy protection. In [16], privacy and heterogeneity challenges in IoT-based smart cities were addressed. An ontology for device heterogeneity and privacy was presented, enabling real-time privacy behavior adjustments. Efficiency was evaluated, showing cost-effectiveness for IoT devices with moderate resources, though scalability issues persisted. In [17], participatory authentication for vehicular edge computing was proposed. It included decentralized identification, blockchain-based group authentication, and secret sharing. The model achieved decentralized authentication, reduced overhead costs, and improved privacy through node cooperation. In [18], the authors focused on health data security in smart cities, addressing the privacy risks of data-based machine learning for medical diagnoses. They introduced LPME, a lightweight mechanism that uses encryption parameters to prevent data exposure and offers timely and private detection. The model demonstrated good security on real-world datasets.

B. Medium-level security threats

The mid-level structure in IoT and smart cities includes a variety of sectors. In fact, in this paper, we consider the network and middle layer the middle layer. We then divided this section into two general sub-sections. In this new division, privacy and data security issues are in one subsection, and communication issues in communication networks in smart cities are discussed in another subsection.

a) Challenges of communication privacy and security in smart cities*:* A new method for outlier detection in IoT data using generative adversarial networks (GAN) is proposed in [19]. Their approach uses an adversarial training paradigm to identify outliers in IoT datasets and enhance anomaly detection capabilities. Using GANs, the model learns to distinguish typical IoT data patterns from outliers, thereby improving detection accuracy. The authors addressed IoT network security in smart cities [20]. They outlined five key factors for effective intrusion detection, introducing a Temporal Convolution Neural Network (TCNN) that achieved high accuracy in traffic detection but lacked IDS flexibility testing. In [21], IDSGAN uses a new framework of GANs to create attacks against IDS. Unlike traditional methods that rely on hand-crafted attack strategies, IDSGAN automates the attack generation process through adversarial learning. Using the capabilities of GAN, IDGSAN can create complex and diverse attacks and challenge the robustness of IDS models. This research highlights the potential vulnerabilities of IDS systems and provides insights into using GANs to assess and improve the resilience of intrusion detection mechanisms. In [22], the authors presented semi-supervised anomaly detection algorithms for IoT communications. They introduced the HS-TCN for detecting abnormalities, showing improved performance in experimental results. In [23], the authors focused on deep learning for identifying IoT attacks. They used a dense random neural network approach to accurately classify seven attack types in the DS2OS traffic tracking dataset, outperforming other machine learning classifiers. In [24], an anomaly detection method based on an iterative convolution autoencoder is proposed for IoT time series data. This approach combines DL and sequential modeling to identify unusual patterns in IoT data streams. This work addresses the critical need for robust anomaly detection mechanisms in IoT applications and ensures the reliability of time series data analysis.

b) Smart city and data security and privacy challenges*:* In [25], the authors addressed data duplication in mobile crowdsensing. They introduced a framework for fog-enabled mobile crowdsensing, improving task allocation accuracy and data confidentiality. The scheme used secure data removal and privacy-preserving techniques to eliminate duplicate data while protecting users' identities. The authors in [26] proposed a security model aimed at 5G IoT services. Their solution uses network slicing to enhance privacy, enabling fog nodes to choose suitable slices while preserving anonymity and protecting data confidentiality. The scheme provided anonymous authentication and secure data channels, enhancing security and efficiency, as demonstrated through simulations. The authors in [27] developed a data aggregation scheme called PLSA-FT, which is lightweight and preserves privacy for IoT devices. However, it was found to be vulnerable to collusion attacks. The authors introduced the LVPDA scheme in [28] for lightweight, verifiable privacy data collection in smart IoT systems. It employed Paillier homomorphic cryptography and online/offline signatures to reduce computational and communication costs, ensuring security during data aggregation. Nonetheless, it was at risk of collusion attacks carried out by malicious users and edge servers. In [29], a user-centric privacy system was proposed for managing personal data in smart cities. The system integrated authentication and privacy mechanisms to support GDPR compliance. It is considered an essential aspect of privacy and security, aiming to minimize personal information disclosure while interacting with service providers.

C. Smart city and cloud security and privacy

In [30], the authors presented a multilayer cloud architecture model featuring a security framework based on ontologies for smart home IoT applications. The model enhanced interactions between diverse devices, services, and applications, offering solutions to heterogeneity issues. The authors in [31] proposed an authentication protocol called TMIS. This protocol ensured the secure exchange of electronic medical records (EMRs) and deduplication of patient data. The framework was verified for security and efficiency, although it didn't cover security aspects during remote patient registration and medical record storage. In [32], a new ABE encryption system, A2B2E, was introduced with hidden access policy features. Users could access data based on group identities and access policies without revealing password encryption policies. However, the scheme should consider preventing malicious users from disclosing decryption information. In [33], a cloud storage system for medical files based on IoT was proposed. It included broken glass access control and secure copying and storage. This system ensured the security of patient's medical records and provided instant access to emergency data, enhancing patient care in healthcare systems.

In [34], the authors introduced an algorithm for resource-constrained IoT devices to run local machine learning algorithms that reduced the need for permanent cloud connectivity. This algorithm maximizes trust in machine learning models through intelligent heuristics while minimizing cloud communication overhead. In [35], a data management system (DMS) for smart cities that uses artificial intelligence modeling techniques to improve privacy and security was presented. The authors highlight the challenges of managing large volumes of data in smart city environments and show how artificial intelligence can model data to preserve privacy and improve security. This system aims to prevent data penetration and optimize data processing in smart cities. Another work [36] presents a protocol for maintaining data privacy in smart cities focusing on energy efficiency. This protocol combines biometric data with a fuzzy scheme to ensure secure data transmission. The authors emphasize the importance of protecting personal data in smart city infrastructure while reducing energy consumption. This protocol is designed for various smart city applications where biometric authentication and privacy are important. In [37], it introduces the SCMC system to measure and control data security in smart cities using data mining algorithms. The authors focus on improving data security in smart city infrastructure using data mining techniques for anomaly detection and predictive maintenance. This system can monitor, measure, and control the city's data in real-time, protecting sensitive information. A secure communication framework for smart city infrastructure is presented in [38], which includes encryption, intrusion detection systems, and blockchain technology. This framework protects communication channels in smart city systems against cyber threats. Blockchain ensures data integrity, and intrusion detection systems help identify malicious activities in real time and increase the overall security of communications in smart cities.

V. Discussion and Results

In the previous sections, the method used to review selected articles on smart city security and privacy management, along with various proposed methods, was fully described. In this section, statistical analysis and comparison of works are considered to determine the appropriate answers to the main questions of this research. In the following section, several analytical subsections are designed to answer the four main research questions and are presented below:

RQ1. What are the most important smart city privacy challenges in the IoT environment?

According to our classification in Section 4, the research concerning smart cities falls into three categories: low, middle, and upper layers of security issues. We analyzed keywords used in relevant research to address our primary research question and identify the main challenges in this domain. Additionally, as IoT and smart city architecture are closely intertwined, many articles encompass various aspects not explicitly mentioned in their keywords. Therefore, we meticulously reviewed these articles and extracted additional critical keywords, which are presented in the statistics in Figure 2. Our analysis indicates that the most extensively studied area pertains to wireless communication, highlighting the substantial attention to securing wireless networks, a vital component of IoT environments. Furthermore, the second most significant challenge identified in this field is related to cloud analysis. This emphasis on cloud analysis is well-justified, as smart cities necessitate data processing in cloud environments equipped with robust storage and efficient analytical capabilities while ensuring the highest levels of security and privacy.

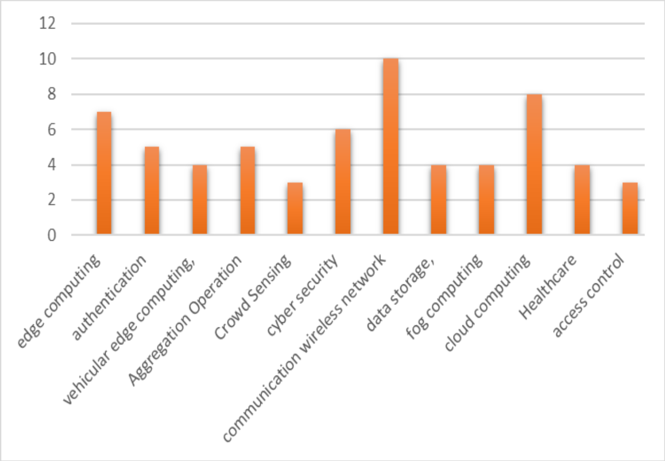

Fig. 2. An analysis of essential issues in the privacy and security of the smart city in the IoT.

RQ2. What techniques have been used to solve IoT privacy issues, and how can they be implemented?

In response to this central question, we classified these methods into five groups, as shown in Figure 3. The most commonly used method, especially in recent papers on different parts of smart city architecture, is using cryptographic techniques with significant focus. The second common category in homomorphic cryptography includes various learning techniques, such as deep and machine learning, in connection with intrusion detection systems. These methods have received special attention, especially in communication security, and have been effective in IoT. The third category includes "other methods". This classification is necessary because these alternative methods, while less commonly used, play a unique role in certain articles. However, including them in the diagram may cause complexity when choosing the most appropriate method. Examples of methods in the "other" category include blockchain, secure hosting, and key transfer.

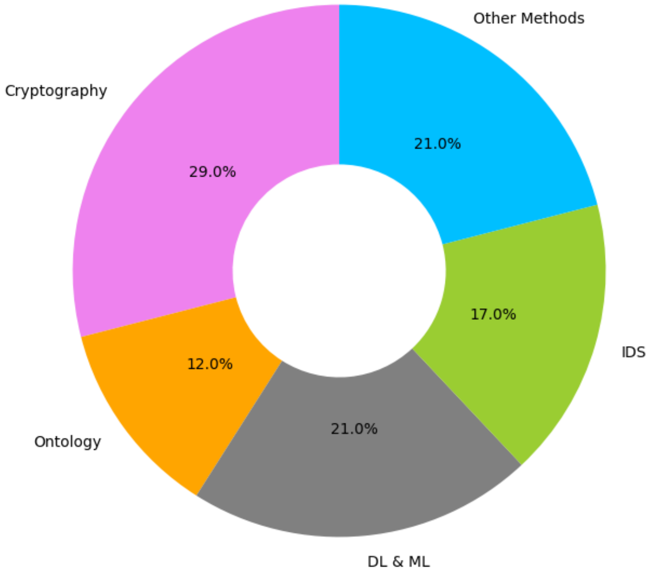

Fig. 3. An analysis of the Main Method in security and privacy problems in smart cities.

According to the diagram in Figure 4 and the study of statistics in the articles, the percentage of implementation and simulation was almost the same. Also, some articles did not discuss implementing and simulating their method.

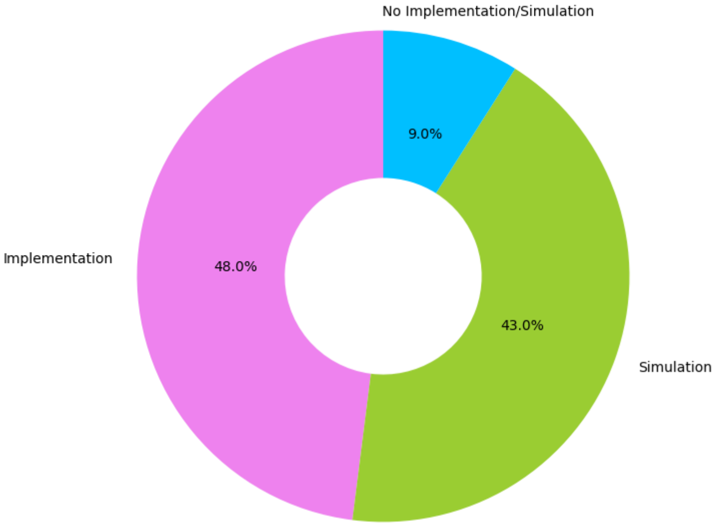

Fig. 4. An analysis of the evaluation environments presented in the reviewed articles.

RQ3. What metrics are essential and can be taken to measure privacy and security in smart cities?

We extracted evaluation factors from our article analyses to address this question to determine the answer. We created diagrams for each defined category, showcasing the main evaluation factors. Figure 5 illustrates the primary evaluation factors for the "physical devices" category. In this diagram, the most critical factor is "overhead," followed by "execution time." These two factors hold utmost importance in assessments due to the limited processing capacity of edge devices. Overhead is particularly crucial for maintaining the privacy and security of physical devices in smart cities.

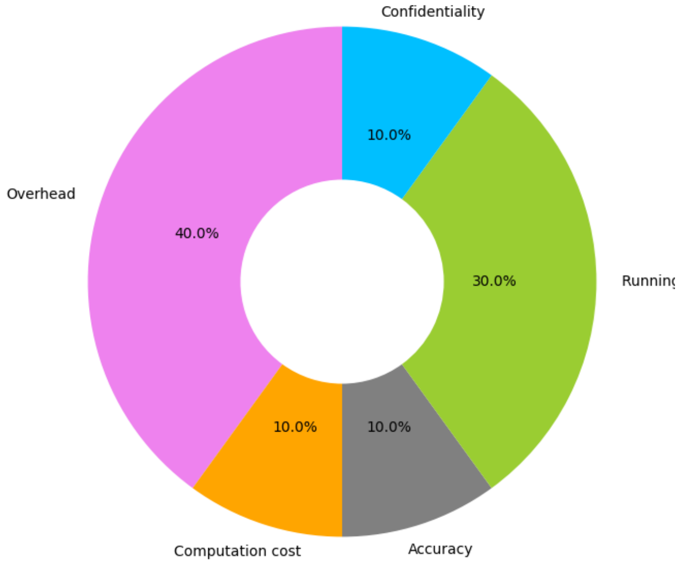

Fig. 5. Evaluation factors in physical devices.

Figure 6 focuses on the key evaluation factors in communication networks. Because many solutions rely on intrusion detection systems, factors like accuracy, precision, recall, and F1-measure have garnered increased attention for measuring system performance. Among these factors, "accuracy" holds the highest percentage in evaluations. Given the security vulnerabilities and potential attacks in these environments, ensuring the accuracy of information received is pivotal for evaluating system implementations.

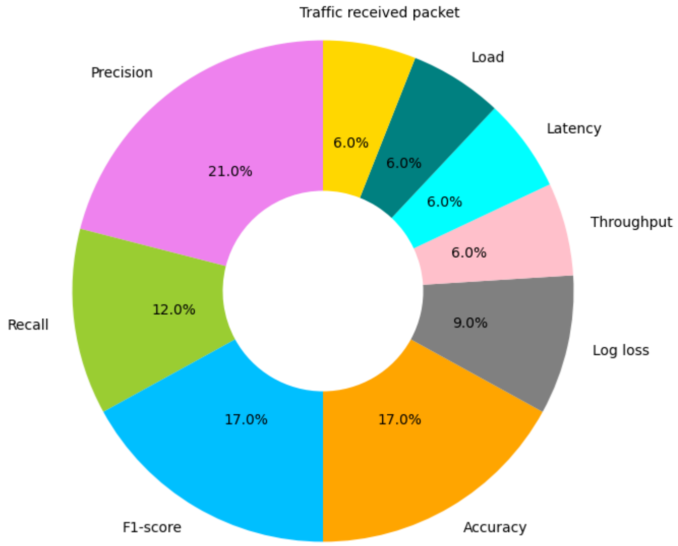

Fig. 6. Evaluation factors in communication networks.

Figure 7 shows the most important evaluation factors in the "data" section. As you can see, most of the articles in this section focus on the "computation overhead", "communication overhead", and "Time cost" evaluation factors. These results mostly discuss privacy and security issues in smart cities. The IoT uses more methods, such as cryptography, which have a high computational and communication load. Also, encryption methods require more time to execute due to their inherent complexity, imposing high time costs on systems implemented with these methods.

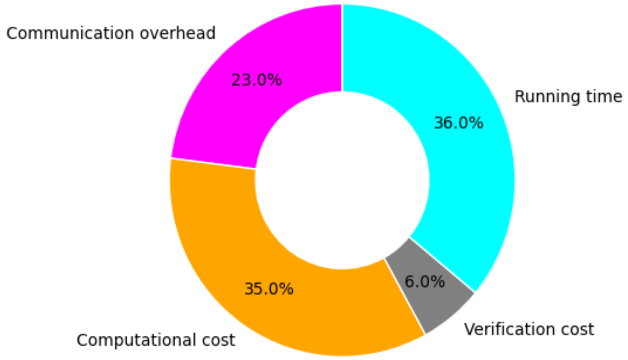

Fig. 7. Evaluation factors in the data section.

Figure 8 provides an analysis of the evaluation factors in the cloud. As you can see, the methods in this section have also evaluated various factors. The reason for this diversity is the use of various methods in solving security and privacy issues at this level of IoT architecture. However, most methods and techniques have used methods based on cryptography and authentication. As a result, the most important factors using these methods and the nature of the clouds are "computational complexity" and "runtime" depending on the degree of security required.

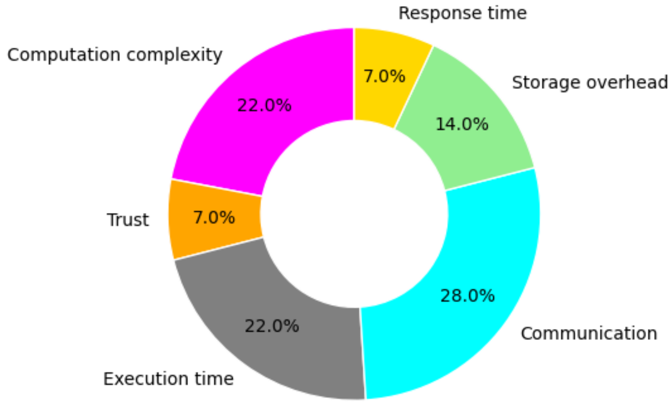

Fig. 8. Evaluation factors in the cloud.

Finally, it should be noted that the architecture of smart cities in the context of the IoT is an integrated architecture. The separation of solutions is difficult and impossible to examine at one level of this architecture. Consequently, a percentage of the combination of solutions should be considered for the categories and reviews presented in this paper and the factors evaluated by the researchers.

RQ4. What are smart cities' challenges, issues, open topics, and future orientations in the IoT context?

To answer this question, we have first presented to demonstrate the importance of the analytical subject based on the year and the subject of publishing the reviewed articles in this SLR. As seen in Figure 11, issues related to privacy and security in smart cities in IoT environments between 2016 and 2022 have been examined based on the resources reviewed in this article. This chart generally shows an increasing slope in publishing articles in this field. In particular, the decline seen in Figure 9 is temporary, and the articles reviewed in this review are up to May 2022, which certainly does not include much of the work done in this area. The general trend is increasing, which shows the issue's importance and the effectiveness of research in this field in the real world.

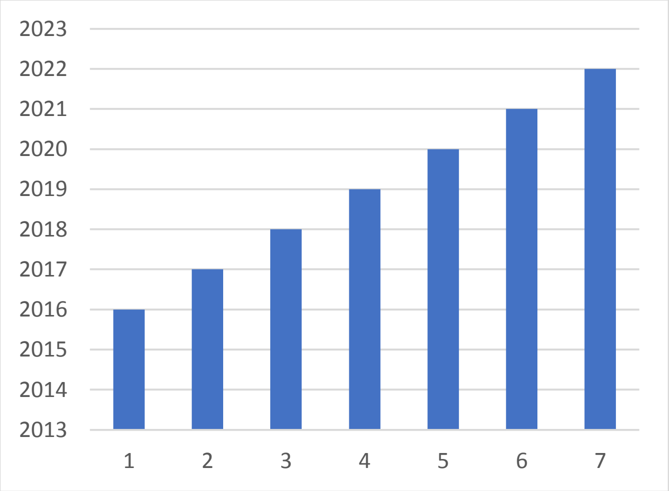

Fig. 9. View of published articles based on the year of publication in the field of privacy and security in smart cities.

We have addressed challenges, open topics, and future goals in four main categories. Table III summarizes these aspects under the proposed classification for better reader comprehension.

A. **Processing limitations in physical devices**: Limited resources and unreliable security mechanisms in sensor devices are significant challenges. These devices are highly vulnerable to security threats, making it imperative to develop lightweight security solutions with low computational overhead and execution time. Ensuring the security and privacy of devices in smart city infrastructures requires energy-efficient security solutions.

B. **Intermediate communication technologies**: Bluetooth, RFID, Wi-Fi, and 4G are communication technologies that can expose vulnerabilities to security threats and intrusions. Ensuring the security of these technologies, including advanced ones like 4G, is crucial to prevent potential security breaches and data compromises.

C. **Cloud layer**: The layer introduces complex privacy and security issues related to outsourcing, big data analysis, and remote access. Data control decreases when outsourcing, and verifiability is essential to ensure data security and privacy. Multi-tenancy in the cloud can create security vulnerabilities that need to be addressed. Additionally, traditional security techniques may not suffice due to the massive volume of cloud data and distributed computing, and new encryption methods may be required to enhance security.

D. **Threats from humans and users' equipment**: Smart city users using mobile devices may expose themselves to vulnerabilities. Mobile phones can be tracked via their International Mobile Station Equipment ID (IMEI), potentially leading to privacy breaches. Users' negligence in granting access to malicious programs can also risk their information and devices. Privacy invasion, data breaches, and other attacks may harm users' privacy and security, necessitating robust protection measures.

These challenges and issues highlight the need for innovative solutions to enhance security and privacy in smart city environments. Table IV presents an overview of open issues, challenges, and future trends across three key layers: physical devices, communication technologies, and the cloud.

TABLE IV. OPEN ISSUES, CHALLENGES, AND FUTURE SMART CITY SECURITY AND PRIVACY SOLUTIONS.

Open issues	Challenges	Future trends
Processing restrictions on physical devices	1. Security solutions with optimal usage of the available resources. 2. Unsuitable and low optimization for large key sizes for encryption/ decryption.	1. Strong authentication for each device in IoT environments. 2. IoT cybersecurity mechanisms. 3.IoT-optimized integrity attestation solutions.

Communication technologies in the middle layer	1. Efficient IoT data storage. 2. Distributed Data Security. 3. Data Privacy and Security.	1. IoT network slicing. 2. Federated learning techniques. 3. Big data-based security solutions. 4. Blockchain-based design.
Cloud layer	1. Weak implementation of encryption. 2. Confidentiality. 3. Leakages. 4. Denial of Service (DoS) Attack.	1. Using Privacy Enhancing Technologies. 2. Using Synthetic Data 3. Using data anonymization 4. Secure multiparty computation

VI. Conclusion

Using the systematic review method, this article examines the research in the field of security and privacy in smart cities and provides a comprehensive understanding of this field. This study reviewed more than 100 articles published between 2016 and 2024. The results of the analysis indicate a significant increase in research on security and privacy for smart cities from 2016 to 2022. Specifically, in response to the first research question, frequent keywords were identified, among which "wireless communication" was raised as one of the most important and challenging topics in the privacy and security in IoT environments in smart cities. Regarding the second question, the analysis and classification of the methods showed that "encryption" was the most common approach to ensure security and privacy in smart cities. In addition, machine learning and deep learning techniques have also been widely used in this field and are known as effective tools in detecting intrusions and improving network security. The third research question addressed the main evaluation criteria at each level of smart city architecture to ensure security and privacy. Criteria such as computational overhead and execution time have been considered in evaluating the security of physical devices and the accuracy and correctness of information in communication networks. These criteria play a key role in improving and evaluating security systems for the complex architecture of smart cities. In response to the fourth question, challenges, open issues, and future research directions were categorized into four main groups. Among these challenges are the processing limitations of physical devices, threats related to communication technologies such as Bluetooth and 4G, and complex security issues in the cloud layer. These challenges indicate the need to develop new security solutions using light and efficient methods that can optimize the limited resources of IoT devices and ensure data security in cloud environments. In addition, due to the increase in the volume of data and the complexity of communication in smart cities, solutions such as using blockchain technologies, federated learning, and fusion cryptography are proposed as promising paths for future research and development. Also, creating resistant mechanisms against new attacks and improving anomaly detection techniques are other necessary paths for future studies. In general, this study not only examines the current challenges and existing approaches in the security and privacy of smart cities but also highlights the future need to develop sustainable and efficient security solutions. Further research in this field can help design and implement safer infrastructure for smart cities and increase citizens' confidence in these technologies.

References

[1] Ogonji, M. M., Okeyo, G., &Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. Computer Science Review, 38, 100312.

[2] Cunha, M., Mendes, R., & Vilela, J. P. (2021). A survey of privacy-preserving mechanisms for heterogeneous data types. Computer Science Review, 41, 100403.

[3] Sarwar, K., Yongchareon, S., & Yu, J. (2018, November). A brief survey on IoT privacy: taxonomy, issues and future trends. In International Conference on Service-Oriented Computing (pp. 208-219). Springer, Cham.

[4] Lau, B. P. L., Marakkalage, S. H., Zhou, Y., Hassan, N. U., Yuen, C., Zhang, M., & Tan, U. X. (2019). A survey of data fusion in smart city applications. Information Fusion, 52, 357-374.

[5] Al- Turjman, F., Zahmatkesh, H., &Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, e3677.

[6] Akil, M., Islami, L., Fischer-Hübner, S., Martucci, L. A., &Zuccato, A. (2020). Privacy-preserving identifiers for IoT: a systematic literature review. IEEE Access, 8, 168470-168485.

[7] Huo, Y., Meng, C., Li, R., & Jing, T. (2020). An overview of privacy preserving schemes for industrial Internet of things. China Communications, 17(10), 1-18.

[8] Safa, N. S., Mitchell, F., Maple, C., Azad, M. A., &Dabbagh, M. (2020). Privacy Enhancing Technologies (PETs) for connected vehicles in smart cities. Transactions on Emerging Telecommunications Technologies, e4173.

[9] Curzon, J., Almehmadi, A., & El-Khatib, K. (2019). A survey of privacy enhancing technologies for smart cities. Pervasive and Mobile Computing, 55, 76-95.

[10] Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet of Things, 15, 100420.

[11] Lau, B. P. L., Marakkalage, S. H., Zhou, Y., Hassan, N. U., Yuen, C., Zhang, M., & Tan, U. X. (2019). A survey of data fusion in smart city applications. Information Fusion, 52, 357-374.

[12] Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2016). Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. *IEEE Internet of Things Journal*, *4*(4), 855-869.

[13] Jayaraman, P. P., Yang, X., Yavari, A., Georgakopoulos, D., & Yi, X. (2017). Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Generation Computer Systems*, *76*, 540-549.

[14] Seliem, M., Elgazzar, K., & Khalil, K. (2018). Towards privacy preserving iot environments: a survey. *Wireless Communications and Mobile Computing*, *2018*(1), 1032761.

[15] Xu, G., Li, H., Tan, C., Liu, D., Dai, Y., & Yang, K. (2017). Achieving efficient and privacy-preserving truth

discovery in crowd sensing systems. Computers & Security, 69, 114-126.

[16] Gheisari, M., Wang, G., & Chen, S. (2020). An edge computing-enhanced internet of things framework for privacy-preserving in smart city. Computers & Electrical Engineering, 81, 106504.

[17] Liu, H., Zhang, P., Pu, G., Yang, T., Maharjan, S., & Zhang, Y. (2020). Blockchain empowered cooperative authentication with data traceability in vehicular edge computing. IEEE Transactions on Vehicular Technology, 69(4), 4221-4232.

[18] Ma, Z., Ma, J., Miao, Y., Liu, X., Choo, K. K. R., Yang, R., & Wang, X. (2020). Lightweight privacy-preserving medical diagnosis in edge computing. IEEE Transactions on Services Computing.

[19] Rani, B. J. B., & ME, L. S. (2020). Outlier Detection in IoT Using Generative Adversarial Network..

[20] Derhab, A., Aldweesh, A., Emam, A. Z., & Khan, F. A. (2020). Intrusion detection system for Internet of things based on temporal convolution neural network and efficient feature engineering. Wireless Communications and Mobile Computing, 2020.

[21] Lin, Z., Shi, Y., & Xue, Z. (2018). Idsgan: Generative adversarial networks for attack generation against intrusion detection. arXiv preprint arXiv:1809.02077..

[22] Cheng, Y., Xu, Y., Zhong, H., & Liu, Y. (2020). Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication. IEEE Internet of Thingsss Journal, 8(1), 144-155.

[23] Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P. K. (2021). Deep neural network-based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Transactions on Emerging Telecommunications Technologies, 32(7), e4121.

[24] Yin, C., Zhang, S., Wang, J., & Xiong, N. N. (2020). Anomaly detection based on convolutional recurrent autoencoder for IoT time series. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(1), 112-122.

[25] Ni, J., Zhang, K., Yu, Y., Lin, X., & Shen, X. S. (2018). Providing task allocation and secure deduplication for mobile crowdsensing via fog computing. IEEE Transactions on Dependable and Secure Computing, 17(3), 581-594.

[26] Ni, J., Lin, X., & Shen, X. S. (2018). Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. IEEE Journal on Selected Areas in Communications, 36(3), 644-657.

[27] Wang, Q., & Mu, H. (2021). Privacy-Preserving and Lightweight Selective Aggregation with Fault-Tolerance for Edge Computing-Enhanced IoT. Sensors, 21(16), 5369.

[28] Zhang, J., Zhao, Y., Wu, J., & Chen, B. (2020). LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT. IEEE Internet of Things Journal, 7(5), 4016-4027.

[29] Daoudagh, S., Marchetti, E., Savarino, V., Bernabe, J. B., García-Rodríguez, J., Moreno, R. T., ... &Skarmeta, A. F. (2021). Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal. Sensors, 21(21), 7154.

[30] Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multilayer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Generation Computer Systems, 78, 1040-1051.

[31] Deebak, B. D., & Al-Turjman, F. (2020). Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of medical things. IEEE Journal on Selected Areas in Communications, 39(2), 346-360.

[32] Xiong, H., Zhang, H., & Sun, J. (2018). Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. IEEE Systems Journal, 13(3), 2739-2750.

[33] Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Information Sciences, 479, 567-592.

[34] Qolomany, B., Mohammed, I., Al-Fuqaha, A., Guizani, M., & Qadir, J. (2020). Trust-based cloud machine learning model selection for industrial IoT and smart city services. IEEE Internet of Things Journal, 8(4), 2943-2958.

[35] Jyothi, V., Tammineni, S., Thiyagu, T. M., Sowndharya, R., & Arvinth, N. (2024). A Data Management System for Smart Cities Leveraging Artificial Intelligence Modeling Techniques to Enhance Privacy and Security. Journal of Internet Services and Information Security, 14(1), 37-51.

[36] Nyangaresi, V. O., Abduljabbar, Z. A., Mutlaq, K. A. A., Bulbul, S. S., Ma, J., Aldarwish, A. J., ... & Neamah, H. A. (2024). Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme. Scientific Reports, 14(1), 16223.

[37] Selvarajan, S., Manoharan, H., Goel, S., Akili, C. P., Murugesan, S., & Joshi, V. (2024). SCMC: Smart city measurement and control process for data security with data mining algorithms. Measurement: Sensors, 31, 100980.

[38] Desai, B., Patil, K., Mehta, I., & Patil, A. (2024). A Secure Communication Framework for Smart City Infrastructure Leveraging Encryption, Intrusion Detection, and Blockchain Technology. Advances in Computer Sciences, 7(1).