ISSN 2614-0047

A comprehensive analysis of IoT security and privacy in smart city applications

Ahmad Anwar Zainuddin [a,1,*], Adam Othman [a,2], Nur Adlin Muhammad Zahid [a,3], Nur Anis Sofea Kamarul Zaman [a,4], Alin Nur Maisarah Ahmad Razmi [a,5], Mohammad Haiqal Azreen Kamarul Zaman [a,6]

[a] Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Gombak, 53100, Malaysia
[1] anwarzain@live.iium.edu.my; [2] adam.o@live.iium.edu.my; [3] adlin.zahid@live.iium.edu.my; [4] sofea.zaman@live.iium.edu.my; [5] alin.maisarah@live.iium.edu.my; [6] haiqal.azreen@live.iium.edu.my
* corresponding author

ARTICLE INFO

Article history
Received August 3, 2023
Revised September 26, 2023
Accepted April 26, 2024

Keywords
IoT Security
IoT Privacy
Smart City

ABSTRACT

With the increasing growth of smart cities, the Internet of Things (IoT) has emerged as a key enabler, integrating various systems and devices to create intelligent urban environments. However, increased interconnectedness raises significant concerns regarding security and for IoT communications privacy. This work addresses the problems with and remedies for IoT connectivity in smart cities that are related to security and privacy. The problems will be addressed by examining the potential risks and vulnerabilities associated with IoT networks, considering device authentication, data encryption, access control, and intrusion detection. Furthermore, an investigation on privacy issues and provide ways to protect sensitive data, such as differential privacy and data anonymization will be conducted. This work further provides a rundown of current safeguarding and discretion practises in IoT communications and highlight new technologies that hold promise for addressing these challenges, based on a detailed assessment of existing research and case studies. Moreover this work outlines important avenues for future study and offer suggestions for strengthening the privacy preservation of IoT communications in the context of tech cities. By solving these fundamental issues, the dependability, sustainability, and trustworthiness of IoT deployments in smart cities can be guaranteed, enabling them to reach their full potential for enhancing the quality of life for urban people.

1. Introduction

Smart cities are rapidly transforming urban landscapes, leveraging IoT technologies to improve efficiency, sustainability, and quality of life. An overview of intelligent city architecture emphasizes the interconnectedness of devices and systems. Furthermore, it introduces the security and privacy challenges that arise in the context of innovative city applications. Open data and pervasive wireless connection will ensure the success of smart cities. The benefits of opening the data vault may be seen in Amsterdam, a well-connected smart city. Over 170 initiatives were part of the Smart City concept when it first started in 2009 [1]. Information and communication technology must engage with lots of physical devices, and there comes a “smart city” to improve the effectiveness of local operations and services and, at the same time, connect with inhabitants. Thanks to innovative city technology, municipal officials may interact directly with the community and city infrastructure, allowing them to monitor what is happening in the city and how it is changing. Information computer technology has greatly cut costs and resource usage and has even improved urban service quality and effectiveness.

"smart cities" applications are developed to manage urban traffic and facilitate quick responses. A smart city may, therefore, be better able to deal with issues than one where inhabitants and the city interact in a more "transactional" way.

The typical resident may not find the technical description of an intelligent city all that thrilling in an urban region where technology and sensors are employed to collect data for resource management. Many people may not be aware that smart city technologies support how individuals will live and work in the future. The technology behind smart cities, such as artificial intelligence and the Internet of Things, represents the future companion. The numerous smart city technologies already in existence and those emerging in the future could lower expenses, increase safety and environmental protection, and improve the quality of life [2]. They could also make services more easily accessible and efficient, reducing citizens' overall carbon footprints. The remainder of this article is organized as follows. Section 2 discusses security and privacy in IoT communications in smart cities. Section 3 outlines the procedure for preparing this paper. Secure Design Suggestion is covered in Section 4. Section 5 concludes this article with Recommendations.

2. Security and Privacy in IoT Communications in Smart Cities: A Literature Overview

This section presents a comprehensive literature overview of at least 15 papers published from 2018 onwards. The table below summarises each paper's key findings and contributions, highlighting the advancements and insights in the field of Security and privacy in IoT communications in urban innovation.

2.1. Urban Infrastructure Design for Smart Cities

Fig. 1 explains the seven layers of the Open Systems Interconnection (OSI) model.

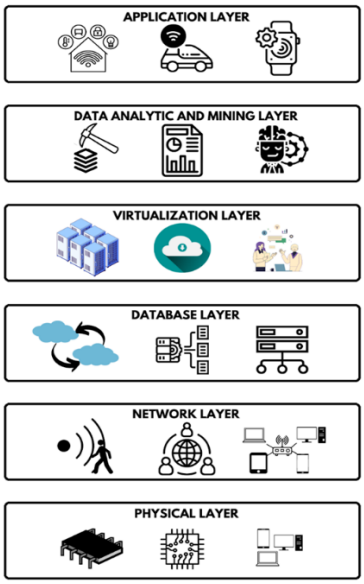

Fig. 1. The layer of architecture of intelligent cities

2.1.1. Physical layer

The lower layer of the architecture, or the perception layer, is the physical layer. This layer incorporates various components, including sensors and actuators, that gather data and transmit it to the architecture's network layer at the top for additional processing [3].

2.1.2. Network Layer

The base element of an IoT-based architecture is the network layer or the communication layer. This layer is not independent and relies on fundamental networks like communication networks, wireless sensor networks, and the Internet [4]. The primary duties of the network layer include connecting servers and other networked devices, as well as sending information that the physical layer has gathered [5].

2.1.3. Virtualization Layer

It creates a single software-based system combining network capabilities with hardware/software, logically changeable entities. A virtual network integration technique is offered by the virtualization layer [6]. For network virtualization to succeed, platform and resource virtualization may be required. This is done by utilizing this layer.

2.1.4. Data Analytics and Mining Layer

Enhancing network efficiency and enabling preemptive identification of future events like system failures are two critical functions of raw data's information analysis and extraction layer transformation into insightful knowledge [7]. This layer employs various procedures and techniques, including machine learning (ML) algorithms, to thoroughly analyze the data and draw out valuable patterns and knowledge.

2.1.5. Application Layer

It is in charge of providing customers with intelligent applications and services that cater to their unique demands. This application layer represents the secure IoT-based architecture's top layer. The following part concisely describes a few common usages [8].

2.2. Practical Use of Technology in Urban Contexs

Urban living is becoming safer and more convenient as IoT-based smart city solutions are implemented. The city's infrastructure and public utility services are being improved. This article will examine the potential of IoT technology, real-world examples of IoT in smart cities, potential advantages, and more. Fig. 2 explains intelligent city applications. A literature overview show as Table 2.

Table.1 A literature overview of Security and Privacy in IoT Communications in Smart Cities

Article	Aim of Study	Summary of Key Findings	Supporting evidence/ Methodology/ Proposed frameworks	Significance/ Contributions
[1]	Examine the effects on society of the dangers and issues resulting from the tremendous advancement of humankind during the industrial era	One of the main conclusions is that cities are crucial to the social and economic fabric of society	- Data Analysis and Assessment - Sustainable Urban Agriculture - Education and Awareness	Discussion of the future role that cities will play in providing their residents with wholesome food. It highlights the pressing need to address food security challenges and provides stakeholders with a roadmap for establishing resilient and sustainable urban food systems
[9]	The study connects educational data mining, activity theory, learning analytics, and activity theory to tackle the problem of forecasting student performance in a collaborative learning environment	Practical student performance prediction models with interpretability are made possible through the integration of learning analytics and HCI theory.	- The study collected data from 1,000 students and used machine learning algorithms to predict student performance based on learning analytics and HCI theory	By shedding light on the connections between learning analytics, human-computer interaction, and student performance, this work contributes to the field and helps to shape personalised learning strategies and educational interventions
[10]	This article's goal is to provide a thorough overview of smart transport systems and the applications for	The primary technologies, difficulties, histories, and architectural frameworks are highlighted in this	A formal, methodical procedure, keyword searches in important databases, screening of 123 articles, final	Future research directions are suggested after a review of smart transport systems. This paper identifies the challenges

Article	Aim of Study	Summary of Key Findings	Supporting evidence/ Methodology/ Proposed frameworks	Significance/ Contributions
	them while assessing technology, communication protocols, and research obstacles	paper's comprehensive overview of smart transportation systems and applications. It examines communication methods and discusses the difficulties of the moment. The direction of future research to enhance these social systems is also highlighted	selection of 87 articles, and backward reference search added 16 more papers resulting in the selection	and difficulties encountered when putting into practise smart transport systems and suggests areas for additional study and development in the area
[11]	The aim of the study is to provide a comprehensive review of the cybersecurity challenges faced in smart city environments. The research aims to identify and analyse these challenges and propose potential solutions to enhance the security of smart city infrastructures	Identification of common cybersecurity challenges. Analysis of existing solutions and their limitations. Proposal of a comprehensive cybersecurity framework for smart cities	The proposed framework involves data pre-processing to collect and integrate real-time data from smart meters and weather sensors. Feature extraction techniques identify patterns and characteristics from the data, while the action selection phase determines optimal	Provides a comprehensive understanding of cybersecurity challenges in smart cities. Evaluates existing solutions and highlights their strengths and weaknesses. Proposes a
[12]	To develop an integrated framework using reinforcement learning for optimising energy consumption and reducing costs in smart homes	Integration of BIM, IoT and blockchain technologies in smart building design allows for improved collaboration among stakeholders, leading to enhanced design coordination and decision-making processes. The utilisation of IoT devices and sensors in a smart building enables real-time data collection, monitoring, and analysis, facilitating efficient building management and optimisation of energy consumption	The study likely employed a combination of literature review, case studies, and theoretical analysis to investigate the application of integrated BIM, IoT, and blockchain technologies in the system design of a smart building. The authors may have examined existing research, industry practices, and standards to identify the benefits, challenges, and potential frameworks for implementing these technologies in a smart building context	This research contributes to smart home energy management by proposing an integrated framework that utilises reinforcement learning techniques. The findings have practical implications for homeowners, utility companies, and policymakers aiming to optimise energy consumption and promote sustainable living. The study also advances the application of reinforcement learning algorithms in real-world scenarios, offering a foundation for future research in smart home energy management

Article	Aim of Study	Summary of Key Findings	Supporting evidence/ Methodology/ Proposed frameworks	Significance/ Contributions
[13]	To conduct a comprehensive survey on the privacy and security aspects of the Internet of Things (IoT), with the aim of identifying vulnerabilities, threats, and strategies to enhance privacy and security in IoT deployments	The survey highlights significant privacy and security challenges in the IoT landscape, including unauthorized access, data breaches, and privacy violations. It identifies emerging trends and technologies impacting IoT privacy and security, such as edge computing and blockchain. Existing frameworks, protocols, and technologies addressing IoT privacy and security concerns are examined, and proposed frameworks and strategies are discussed.	The study employs a comprehensive survey methodology, analysing data from academic research papers, industry reports, and standards and guidelines. It explores common privacy and security issues in IoT and examines existing frameworks, protocols, and technologies. Proposed frameworks and strategies are suggested to strengthen IoT privacy and security.	This study contributes to understanding the privacy and security challenges in the IoT domain. It emphasises the need for robust measures to safeguard IoT devices, networks, and user data
[10]	The article aims to address the weaknesses of weak keys as well as the possibility of unauthorised usage, remote keyword crimes, and lost or missing devices	The suggested dual authentication and credential negotiation mechanism ensures secure access to the device's confidential data. When compared to existing protocols, the protocol improves protection against relevant security attacks and provides a lower communication overhead	- Formal security examination. - Enrolment process with a Registration Server (RS) and secure access using one's identity, a username and password and biometric details. - The protocol negotiates with the RS a session key, which is used for protecting the files on the storage device	The research addresses the shortcomings of low entropy passwords and presents a way to improve the safety of consumer storage devices. The suggested protocol allows for secure access to personal information while also protecting against various security threats. Also, the study adds a formal security analysis based on BAN logic
[14]	The research focuses on the applications, benefits, problems, and futures of machine learning approaches for enhancing medical facilities in smart cities	Smart healthcare systems based on IoT, and machine learning enable personalised and remote care, increasing patient outcomes and lowering healthcare expenditures. Machine learning algorithms are capable of effectively analysing data from sensors from smart watches and other IoT devices to deliver important conclusions for pre-emptive and	- Conducting a thorough review of relevant papers published in academic journals and conference proceedings. - Find and analyse publications highlighting the use of machine learning techniques in smart healthcare in the context of IoT-enabled smart cities. - Present frameworks or models that demonstrate	The findings add to existing knowledge by demonstrating the possibilities of machine learning algorithms to revolutionise healthcare delivery and improve patient outcomes in the setting of smart cities. The insights in the article can help policymakers, healthcare practitioners, and researchers adopt machine learning approaches to optimise

Article	Aim of Study	Summary of Key Findings	Supporting evidence/ Methodology/ Proposed frameworks	Significance/ Contributions
		proactive healthcare management.	how machine learning algorithms	healthcare services and encourage the growth of smart cities with better healthcare architecture
[15]	In the standard privacy protection model, the study addresses the prisoner's dilemma, and it develops a non-constant repeating game model to analyse the tactical negotiations between a third-party visitor and a privacy protector.	The study proposes a security strategy based on the visitor's level of tolerance for confidential information leaking and the likelihood of a genuine visit. The user-specified privacy protection threshold decides whether an access request is granted. The study also examines the dynamic adjustment of the threshold based on network environment and privacy concerns	The creation of a game theory-based model that considers the visitor's access request, historical access records, and the computation of rewards based on various methods	Providing a framework for safeguarding geographical data privacy in LBS applications. The proposed architecture allows users to safeguard their confidential data while yet allowing visitors with good intentions to gain access. The study helps advance the field of privacy protection in location-based services by resolving the difficulties of privacy breach tolerance, access management, and strategic interactions between users and visitors
[16]	The objective of this survey is to offer a thorough understanding and broad perspective of the most recent research works made available to the public about the PLS of key technologies to be deployed in forthcoming 5G wireless networks	Physical layer security (PLS) has demonstrated to be the most effective method for securing upcoming 5G networks, owing to its low complexity and easily implemented techniques in comparison to cryptographic schemes.	According to Liu et al. (2016), secure communication systems that employ physical layer security (PLS) techniques can be evaluated using various performance metrics that consider distinct aspects of secrecy and reliability	The comprehensive review highlights the current state of research in PLS and provides insights into future research directions to enhance the security of emerging technologies
[17]	The study emphasized various security aspects concerning smart homes that connecting to digital era	Some of the generic security measures that must be implemented for the Internet of Things are good and updated software, authentication, authorization, encryption, having physically of security. The IoT and smart city security architecture are	The evidence is a denial-of-service (DoS) attack aims to block a communication channel by occupying it and increasing the chances of collision	The statement highlights the critical security concerns surrounding the industrial IoT devices and emphasizes the need for future studies to focus on specific characteristics, such as privacy protection and terminal security, to develop robust IoT security systems

Article	Aim of Study	Summary of Key Findings	Supporting evidence/ Methodology/ Proposed frameworks	Significance/ Contributions
		driving the expansion of PIoT.		
[18]	The goal of this study is to create a model of a smart home network using fog computing while to make the smart home secure and protected. It can keep it safe, like locks and alarms	In this paper, the authors discuss a unique method for IoT devices in a smart home to securely share secret codes. They employ a technology called fog computing to enable this secure communication	To establish a secure and safe keeping communication bridge, there is a special device ID required to connect with the chosen key. Without the key, System Administrator will facing major problems to ensure that devices communicating with the correct fog server	The research addresses the concern that industrial IoT devices are sometimes used in locations where there is no human supervision, necessitating the assurance of their safety. Ensuring their security is not always easy as the devices themselves lack significant power or resources to protect themselves
[19]	Challenges of Mobile Crowd Sensing and propose solutions	One of the most important discoveries is that many apps do not employ a secure communication channel to transport sensor data from the user's mobile device to the server.	- Sensing applications - Dynamic Analysis Tool - Testing method	During mobile sensing, sensed data (location and motion data) is encrypted and authenticated before being transmitted to their respective servers
[20]	Research on how to ensure privacy preservation concerns during big data exchange	While both sides are engaged in the big data exchange process, one does not like that the partner has access to sensitive areas of the huge dataset	A case study during the Covid-19 era involved two hospitals, H1 and H2, where patients were first screened at H1 and then at H2. H1 needed to share its large clinical dataset from the initial screening campaign with H2. (H2 was not happy that their sensitive classified information may be accessed)	The proposed decentralised solution for big data exchange enables direct data sharing among participants using blockchain technology, eliminating the need for intermediaries. It provides secure transaction recording and enables data owners to monitor data usage in order to safeguard intellectual property and privacy.
[21]	Security and privacy concerns with IoT	This study presents a cyber security architecture for the IoT-based EI that considers the smart grid's existing security challenges.	- Identity-based security mechanism (I-ICAAAN) - Secure communication protocol and an Intelligent Security System for Energy Management (ISSEM)	The proposed frameworks address smart grid security concerns by identifying attacks, applying security measures, building secure communication protocols, improving energy router security, and utilising a cybersecurity framework for scalable vulnerability analysis and resolution

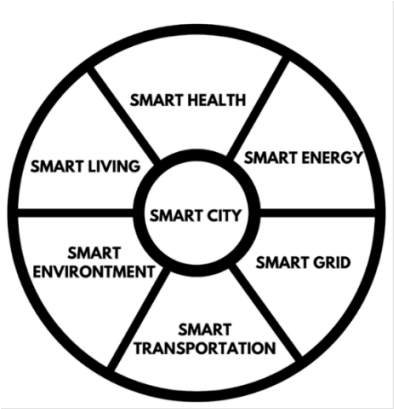

Fig. 2. Smart City Uses

2.2.1. Smart Transportation

In intelligent transportation, there are seven classes based on their functions :

- Route Optimization

  Route optimization is a powerful technique that improves productivity, lowers expenses, and increases customer happiness. It develops the most effective routes that expedite operations and enhances overall performance by considering variables like distance, time, and resources.

- Parking

  A gateway device is put in place next to the road to gather data and send it to a distant server. The system uses magnetic sensors to recognize when vehicles are in parking slots. The system considers all the acquired information when a parking request is made. The best parking possibilities are then chosen for the customer by a cloud-based software agent.

- Lights

  Smart streetlights (SSL) are crucial for smart cities and mobility. Using IoT technology, SSL enables dynamic changes to light intensity in crowded locations. For maintenance, GPS enables position tracking [22]. Using light and IR sensors managed by a Raspberry Pi, Kokilavani and Malathi streamlined the design. For cost savings and improved safety, the system can also serve as a Wi-Fi hotspot, monitor surroundings using cameras and sensors, and adjust illumination based on the environment.

- Controlled Junction and Traffic Light

  Traffic lights are essential to govern controlled junctions where cars are allowed to enter. Sensors are frequently used to control traffic lights. By carefully synchronizing traffic lights, Intersection control seeks to maximize junction throughput and minimize stopping time by regulating the speed of approaching vehicles. An intersection control agent efficiently controls traffic lights, and more significant regions can be governed by cooperation between several intersecting agents [23].

- Accident Detection

  Every community should place a high premium on accident detection and prevention because a successful preventative plan can save lives. Accident prevention relies heavily on a method that warns drivers of emergencies and permits quick intervention. Machine learning, which is especially good at tracking accidents and seeing trends, can foresee probable crashes and alert drivers in advance so they can take preventative action and avoid them [24].

- Road Anomalies

  Road anomaly detection is essential for intelligent transport since it directly impacts many different areas. Finding potholes and bumps aids in avoiding accidents, automotive damage, and backed-up traffic. With 98% accuracy, a CNN-based technique recognizes concrete fractures in images with poor lighting [25]. Without data augmentation or pre-processing, crack damage

detection in UAV images is made possible using transfer learning and deep learning models that have already been trained and attaining up to 90% accuracy in practical situations. For increased road safety, these methods improve the detection of road anomalies.

- Infrastructure

  Modern transport has been transformed by IoT technology, which has allowed for new applications and enhanced systems. Intelligent Transportation Systems are improved by employing an M2M-based architecture for vehicle-to-vehicle communication concepts. Cars communicate speed, motion, and position information, warning approaching traffic of rapid speed changes and exchanging congestion information for better navigation. An IR sensor, RFID tag, and GPS-based bus fleet monitoring system collect data and upload it to a cloud server [26]. The Vehicular Social Network Protocol (VSNP), which is cross-layered, is used by the Social Internet of Vehicles (SIoV), which combines social networks with IoT.

2.2.2. Smart Environment

Our surroundings are essential to the idea of an intelligent environment, and one typical problem that individuals encounter is high electricity costs. The existence of motion sensor addresses this LED lights, which enable users to use less electricity. These lights only turn on when movement is sensed to conserve energy when there is no activity [27]. Intelligent sensors monitor water contamination, air quality, and river levels to prevent floods, making cities safer and more sustainable. Weather sensors can also automate irrigation systems and find leaks.

2.2.3. Smart Living

The use of technology in numerous facets of daily life is referred to as intelligent living. It entails utilizing networked devices and systems to boost comfort, effectiveness, and sustainability. Automation and IoT technology are used in smart homes to regulate the lighting, temperature, Security, and appliances. Wearable technology and fitness trackers encourage healthy behavior by monitoring vital signals. Systems for managing energy use optimize energy use while lowering costs and environmental effects. Smart living promotes a connected, efficient lifestyle that provides convenience, safety, and environmental friendliness, enabling people to lead wiser and more sustainable lives [28].

2.2.4. Smart Health

By utilizing networked infrastructure and sensors, innovative health in smart cities seeks to transform the healthcare industry. Early detection of contagious illnesses, including the flu, colds, and chickenpox, is made possible by real-time data monitoring, which enhances patient care. Smart health offers remote consultations and medical monitoring for people with chronic conditions. Applications that use the cloud can access and examine health data, including signals from fitness smartwatches and other wearables like electrocardiogram (ECG) and electrical impedance tomography (EIT) signals. Technology is used in this redesigned healthcare method to improve well-being and provide individualized treatment [29].

2.2.5. Smart Energy

Sensor nodes are essential in intelligent cities for tracking energy production and consumption and guaranteeing effective resource management. Energy usage is significantly decreased through intelligent energy solutions, including integrating smart grids and infrastructure for electric vehicle charging. Utilizing these technologies makes it feasible to improve personal energy efficiency, avert power grid outages, and optimize energy use. This comprehensive strategy for intelligent energy encourages resilience and sustainability in the urban setting, fostering a greener and more dependable energy ecology [30].

2.3. Protecting Data in the Era of Smart Urbanization

The task of transforming an entire city into a smart city is not simple; it presents significant challenges rather than being rreadily achievable. Such cities heavily rely on multiple layers, including data/information, technology, application, and infrastructure, which complicates security and poses considerable challenges. In the subsequent section, the primary security and privacy concerns involved in making a city bright will be delved into.

2.3.1. Infrastructure Security

In transforming a city into a smart city, the cyber-physical infrastructure encounters various risks and vulnerabilities. The implications of inadvertent threats on a smart city are contingent upon the level of maturity and intelligence achieved by that city. Electricity supply, water distribution, roadways, buildings, and other urban infrastructure confront security vulnerabilities in their respective cyber-physical components and systems.

- Cameras

  In smart cities, a wide array of cameras, both public and private, are deployed throughout residential areas and roadways. These cameras are typically secured through encryption or username and password protection. However, there is a concern that malicious actors may compromise the security of these cameras, gaining unauthorized access and exploiting them for personal purposes. Such breaches can lead to serious privacy violations, particularly for organizations, including government entities.

- Communication Network

  Intelligent cities utilize various communication technologies, including Wi-Fi, 4G, RFID, GSM, and other similar technologies, to establish connections between cyber-physical objects. Each communication technology poses specific security concerns that must be addressed during deployment and usage. It is essential to consider the potential vulnerabilities and threats associated with each technology to ensure the Security of the communication networks within the smart city.

- Building Management System

  Transportation management systems, especially those governing air traffic or train control, are highly susceptible to significant cyber breaches. As a result, manufacturers may not offer notification options to inform consumers of security violations, nor do they resolve vulnerabilities quickly. This leads to insecure and inadequately protected building management systems vulnerable to possible breaches.

- Transport Management Sustem

  Transport management systems are particularly vulnerable to severe hacks, especially regarding air traffic or train control systems. Breaches in these systems can lead to catastrophic consequences. Additionally, hacking control systems of traffic lights, road signs, and speed limit signs can cause significant traffic disruptions lasting for hours. These vulnerabilities highlight the need for robust security measures to protect transport management systems from potential attacks [31]. Fig. 3 indicates the security issues, which can be divided into two parts.

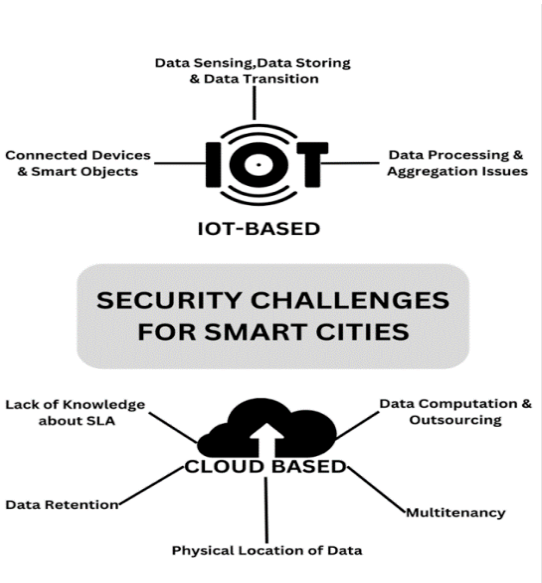

Fig. 3. The security issues can also be divided into two parts: IOT-based and cloud-based

2.3.2. Connected Devices and Smart Object

Collecting excessive data can infringe upon individuals' privacy. The challenge lies in balancing collecting necessary data for innovative city services and respecting privacy rights. Implementing robust data anonymization and aggregation techniques can help mitigate privacy concerns [32]. Inadequate data protection measures can lead to security breaches, compromising sensitive information. Lightweight cryptographic algorithms must balance security and resource efficiency to ensure data confidentiality and integrity without overwhelming IoT devices' limited capabilities [33].

2.3.3. Data Sensing, Data Storing, and Data Transition

Secure storage entails safeguarding data while it is at rest to avoid unauthorised access, manipulation, or data breaches. Encryption, access controls, and secure protocols are used in the context of smart cities, where enormous amounts of sensitive data are gathered and stored. Access restrictions limit access to authorized people or systems, while encryption makes sure that the stored data cannot be accessed without the proper decryption keys [34]. Transaction logging refers to the process of recording and storing information about various actions or events that occur within an IoT system. This includes data on device activities, user interactions, system events, and communication transactions. Transaction logs serve as an audit trail that can be used for troubleshooting, forensic analysis, compliance, and accountability purposes [12].

2.3.4. Data Processing and Aggregations Issue

Transaction logging is recording detailed information about actions and events within the IoT system. It serves as an audit trail, providing visibility into system operations and access patterns. Transaction logs are crucial for detecting security incidents and investigating anomalies. However, improper or insufficient log protection may present privacy and security risks. The integrity of the auditing process might be jeopardized, and privacy violations can result from tampering with logs or unauthorized access to sensitive data they contain [35]. Data validation and filtering are essential to maintain data integrity and lower the possibility of security and privacy assaults. These processes verify the precision, comprehensiveness, and consistency of the data. They filter out irrelevant or unnecessary data, reducing the risk of unauthorized access or misuse of sensitive information. However, improper implementation or insufficient validation and filtering measures can have adverse effects. Ineffective data filtering or inadequate validation can lead to the retention of irrelevant data or acceptance of incorrect or malicious data, compromising the integrity of analysis, decisions, and system security [13].

2.4. Smart City Environment Safety and Confidentiality Approaches

Several solutions have been offered to overcome the security and privacy challenges. This section overviews current methodologies, including encryption techniques, access control mechanisms, anomaly detection methods, and privacy-enhancing technology. Fig. 4 depicts the solutions for innovative city environment safety and secrecy.

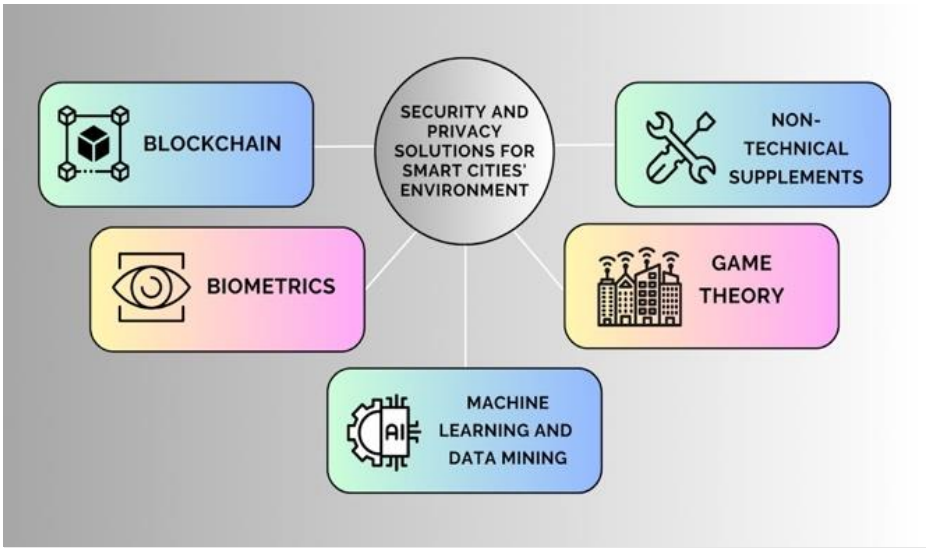

Fig. 4. Smart City Environment Safety and Confidentiality Approaches

2.4.1. Blockchain

While blockchain computing has been a hot topic in recent years, leading to more reliable and helpful software, it is still in its early phases in the Internet of Things era. Steps must be taken to utilize this technology more effectively to address severe privacy and security concerns. Privacy, mutual dependency, efficiency, and openness are essential Blockchain qualities that can be applied to the construction, deployment, and oversight of intelligent city infrastructure. One of the core objectives of Blockchain is to get rid of intermediates to achieve sustainability.

In 2016, Biswas et al. developed a blockchain security architecture that can secure the data transfer confidentiality of urban intelligent gadgets while increasing system dependability and efficiency [36]. Dorri et al., on the other hand, introduced blockchain computing into the context of smart homes in 2017, and the recently formed structure can satisfy the objectives of Security, reliability, and accessibility [37]. They combined the advantages of Blockchain with cloud computing and networking software-defined (SDN) technologies to develop an innovative distributed framework that achieves its architectural objectives of durability, productivity, adaptability, flexibility, and confidentiality.

Furthermore, blockchain technology has been effectively used in intelligent city businesses. Among the positives, present techniques of blockchain-assisted intelligent city systems have significant drawbacks, such as scalability issues, insufficient storage capacity, increased processing, and time. As a result, the demand for creative and new blockchain solutions is growing.

2.4.2. Biometrics

Biometrics are frequently employed in IoT-based system validation. This technology could recognize humans based on biological characteristics and distinct behavioral characteristics. Faces, fingerprints, digital signatures, voices, and other biometrics generate biodata. A possibility worthy of highlighting is brainwave-based verification, which may attain great recognition precision while being effective [38].

Biometric sensors such as digital fingerprints, programs for facial recognition, and iris scanners are used to identify people based on their unique physical characteristics. This technology is used to secure public spaces, enhance access control, and track people's and commodities' movement. Biometric sensors are increasingly being used in smart city security. They verify access to restricted places such as buildings, cars, and other regions. The sensors can also detect and track people in public areas, allowing officials to track and respond to possible threats.

To safeguard vital consumer information via storage media, Amin et al. proposed a mutual identification and critical negotiation method [39]. Compared to similar systems, the novel protocol efficiently resists security breaches while reducing transmission overhead and cost. According to Natguanathan et al., the need arises to build confidentiality biometric systems (PPBSs), similar to the study conducted by Wang et al. They also forecast a promising future for biometrics in various fields, including e-commerce.

2.4.3. Data Analysis and Machine Translation

The fields of artificial intelligence and machine learning, combined with an IoT-enabled Wireless Sensor Network (WSN), can substantially contribute to the healthcare situation, whether in disease prevention, early diagnosis, or therapeutic selection [40]. Better and more tailored medical treatment can be delivered in the future. Artificial intelligence relies heavily on machine learning. It necessitates a significant amount of sample data, from which sophisticated algorithms using pattern recognition construct models.

A recent study created an inventive extraction and selection of features model with a high detection rate for detecting attacks on Wi-Fi networks. According to network security centers, specific machine learning (ML) algorithms have been used in the past decade to analyze, anticipate, and make tailored choices [14]. The rapid development of sensor networks and cell phones has prompted various privacy and security concerns among citizens. Lee et al. employed SVM to develop a multi-sensor verification system for smartphone users. The basic idea was to learn about consumer habits and the variables influencing them.

A comprehensive investigation done by Tsai et al. in the context of data mining (DM) revealed that large amounts of data received by multiple technologies and sensors surrounding people are

mined to discover new regulations and data to provide enhanced amenities [41]. However, DM technologies have safety and confidentiality issues because private data may be shared, including where users are and habits.

2.4.4. Game Theory

In addition to several application scenarios, game theory is effectively used in the fields of safeguarding privacy and cybersecurity. Do et al. conducted a thorough study establishing the game-theoretical method's characteristics and advantages over standard defense mechanisms such as prompt action, dispersed solutions, proven mathematics, and trustworthy defense.

La et al. created an action theoretical framework to investigate the threat and prevention dilemma in honeypot-enabled systems [42]. The concept could be modified to new emergent IoT applications, including intelligent health care, intelligent buildings, and sensor networks. In terms of privacy, the concept of games with other privacy-protecting methods, such as the principle of k and asymmetrical confidentiality, to develop mechanisms. Furthermore, game theory is an efficient tool for balancing the severity of protection with the utility of data.

In terms of privacy, a growing body of research combines the concept of games alongside current anonymity-protection technology, such as the concept of k and differential confidentiality, to develop mechanisms [43]. Furthermore, as Xu et al. argued in 2015, game theory can be used to balance protection intensity with data value [44].

Even though less research has been conducted to apply game theory to specific intelligent urban uses, many innovations are being developed across the field of Security for the Internet of Things. It is anticipated that with the rapid development of everything-connected urban areas, game-theoretic approaches will play an essential role in resolving sure Security and privacy issues of the intelligent era.

2.4.5. Non-Technical Supplements

Protection cannot be provided solely through technical means. Existing technological limits can be reduced by strengthening regulations, legislation, governance, education, etc.

A sustainable innovative system requires good governance. According to Walravens, the government must carefully analyze who has access to the data and what kind of data can be evaluated [45]. Simultaneously, Batty et al. proposed that the government's law should protect model development and data under an intelligent city framework [46].

It is also vital to train suppliers, vendors, and customers to increase their necessary skills. For example, training should assist application designers in writing robust and long-lasting code. Repairing flaws in firewall software is the responsibility of vendors. Furthermore, equipment manufacturers ought to do everything in their power to raise the overall safety and quality standards.

The goal of education programs is to raise citizens' awareness of how new apps work as well as techniques for staying safe. However, effectiveness continues to be a difficulty. Aleisa and Renaud discovered that, while being informed of the risks of privacy leakage, some users disregard their worries in favor of usability [47].

3. Method

This research paper intends to give an in-depth review of relevant literature on the topic of Security and Privacy in IoT Communications in Smart Cities. The approach taken in this study includes a systematic strategy for identifying, selecting, and analyzing scholarly papers that contribute to the understanding of the research issue. The following measures were taken:

3.1. Identification of Relevant Articles

Comprehensive Literature Search: A thorough literature search was conducted to identify articles related to the research topic. Keywords and search terms included [Architecture of Smart Cities, Applications of Smart Cities, Security and Privacy Issues in Smart Cities' Applications, Smart City Environment Safety and Confidentiality Approaches, Recommended Secure Architecture, and Areas Requiring Deeper Exploration].

Articles were reviewed for inclusion and rejection based on previously established standards. Inclusion requirements include articles written in English, published during the last eight years, and specifically centered on the subject matter of the study topic. Articles that did not relate to the research goals, like those that were not peer-reviewed or full-text accessible, were excluded.

3.2. Screening and Selection Process

Title and abstract screening: The screening process starts by reading each article's title and abstract to determine how relevant it was to the study question. During this stage, articles that did not fit the criteria for inclusion were excluded.

Full-Text Review: a comprehensive full-text review was conducted on all of them to decide if the remaining articles were appropriate for inclusion in the review. Each article was evaluated for its substance, research techniques, and applicability to the study's goals. The researchers discussed and agreed on any differences or uncertainties.

3.3. Quality Assesment

criteria. This involves evaluating each article's overall methodological reliability, the findings' validity, and the study design's accuracy.

Risk of Bias Evaluation: All potential biases or limits in the included publications were carefully examined and debated

3.4. Synthesis and Reporting

Findings Synthesis: The findings from the chosen publications were synthesized and organized to give a convincing narrative and a thorough grasp of the research issue. The literature's similarities, differences, and gaps were emphasized and explored.

Reporting: The rules were followed while reporting the review's findings. The review's methodology, conclusions, and implications were clearly described.

4. Secure Design Suggestion

A city design that relies on highly modern technology to make it intelligent and efficient currently relies on millions of resource-limited devices and HetNets to operate [16]. There are some core elements of this architecture, including unified communications (UC), a trusted software-defined networking (SDN) controller called TTP, black networks (BNs), a key management system (KMS), and a registry (UR). There are some core elements of this architecture, including unified communications (UC), a trusted software-defined networking (SDN) controller called TTP, black networks (BNs), a key management system (KMS), and a registry (UR). The Fig. 5 explains the various parts that make up a secure architecture for smart devices by high technology.

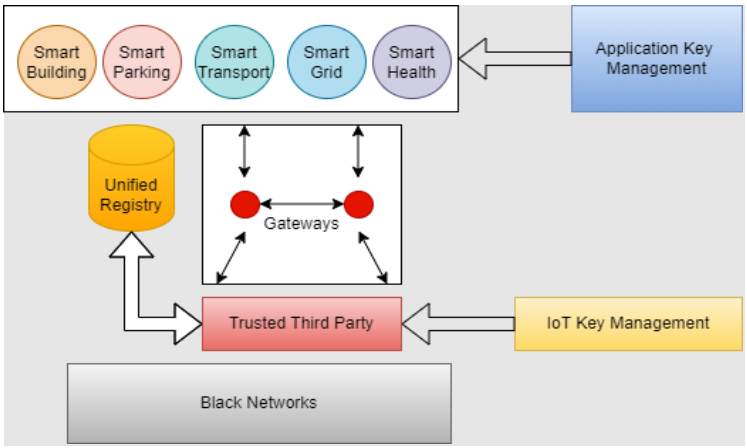

Fig. 5. Summarizes the various parts that make up a secure architecture for smart devices by high technology

- Black Networks

  In an IoT protocol, black networks are used to secure the meta-data of each packet [17]. Other encryption algorithms such as RSA or ECC can also be used to safeguard the data, depending on

specific needs. It is crucial to select the proper encryption method based on the specific objectives and the amount of Security required for the smart devices' infrastructure. It offers authentication and secure communication at both the network and link layers. As a result, this approach effectively reduces active and passive threats, guaranteeing confidentiality, privacy, and integrity in IoT networks.

- Trusted SDN Controller

  The architecture of software-defined networking presents numerous possibilities for improving network security. In this approach, an SDN controller facilitates communication between network devices through various protocols, with OpenFlow being the most used protocol [48]. The SDN controller's primary goal is to handle routing concerns connected to privacy protection in IoT-based BNs. Using the OpenFlow protocol, the SDN controller can establish a safe link to network devices [11]. By incorporating a reliable SDN controller, it becomes feasible to maintain a holistic perspective of the IoT network and effectively manage sleep and wake cycles.

- Unified Registry

  The primary goal of UR is to establish IoT networks for smart cities by integrating diverse technologies. It also includes a mobile feature for cross-system IoT nodes to enhance its purpose. Security is a significant factor in IoT networks that use fixed nodes and wireless communication technologies like Wi-Fi and Long-Term Evolution [49]. Innovative environments utilize multiple addressing techniques, including IPv6 128-bit addressing, radio frequency identification addressing, and Bluetooth 48-bit addressing, on protocols like ZigBee, Bluetooth low energy, and others [50]. UR strives to create a unified platform encompassing identity management, authentication, and authorization across all technologies, protocols, and schemes. Additionally, UR is vital in facilitating wireless communication technology, protocol, and addressing technique conversion.

- Key Management System

  The management and Security of cryptographic keys are vital components of any security system, particularly within IoT ecosystems where limited resources and devices rely on symmetric shared keys to communicate securely [18]. Ensuring the proper distribution of keys is a vital concern, addressed explicitly by the hierarchical Key Management System (KMS) for symmetric keys in intelligent cities. Given the diverse security concerns across IoT applications, various security methods and standards are necessary to address their unique requirements. Commonly used IoT protocols lack inherent security mechanisms, but incorporating protocols like Constrained Application Protocols (CoAP) can enhance their Security by leveraging protocols like Secure Sockets Layer (SSL) and others. Two-factor authentication is critical to be used to ensure the secured communication between IoT devices. By employing this method, the risk of security breaches can be effectively mitigated.

  To enable efficient routing, SDN controllers can construct flow tables for packets that require transfer. This ensures the availability and synchronization of nodes, facilitating seamless communication. UR takes charge of nodes' authentication, authorization, and identity management. Additionally, KMS offers external key management to facilitate secure communication among IoT nodes by utilizing a shared key. Table 2 explains the recap of security services and components used by intelligent cities that rely on modern complex technologies.

Table.2 Recap of security services and components used by intelligent cities that rely on modern complex technologies

Components	Services
Black Network	Routing functions, directing network traffic between different devices and networks
Trusted Third Party	Offer critical management services, such as generating and distributing cryptographic keys for encryption and decryption.
Unified Registry	Help assess the safety requirements and compliance of robotic systems in various environments. n

4.1. Areas Requiring Deeper Exploration

Despite the progress in addressing security and privacy concerns in smart cities, several open issues remain. This subsection discusses the current limitations and outlines potential research directions to enhance further the safeguarding of IoT communications in urban innovation hubs.

- Mobile Data Collection

  Mobile Data Collection is the technique of gathering data from many people using mobile devices, often smartphones, to obtain information about the environment, events, or trends. It involves utilizing the sensors and capabilities of mobile devices and user participation to construct a collective sensing network and collect data for various purposes, such as tracking the environment, urban planning, or social studies [51]. Even though mobile crowd sensing has various benefits that might improve people's quality of life, data trustworthiness is a crucial concern because collected data is frequently utilized for decisions that affect citizens' quality of life. One the example of an application that uses mobile crowdsensing is a navigation application called ‘Waze’. Waze utilizes this feature by collecting user reports about traffic, accidents, police sightings, and roadblocks. Waze also uses the GPS feature on users’ smartphones; hence, this leads to the concern of being tracked by another person with an ill intention.

- Big Data

  Big data is a collection of data that is growing in volume exponentially with time [52]. Big data is gaining popularity in the context of next-generation applications and systems due to the nonstop development of technology. Without a doubt, the privacy of big data is a primary research focus, as it raises issues regarding who owns the data and who has access to it [53]. There are many applications that use the big data concept in collecting user’s personal information. One example of a mobile application that uses this concept is a period tracker app called ‘Flo’. Flo collects users–women’s information about their period dates and symptoms to help users track and manage their menstrual cycles. In July of last year, this Flo app was served with a court order for breaching a private and secret agreement with a third party by selling users' data to the government. This is proof that big data privacy concerns are not something that should be taken lightly.

- IoT Authentication and Authorisation

  In basic terms, IoT is a vast network of interconnected devices that can communicate information and perform activities without requiring direct human intervention [54]. Because of the complexity of the IoT, developing an exceptionally secure and efficient framework for detecting and preventing security vulnerabilities is difficult [55]. Unlocking a car with a smartphone is one example of IoT. In this example, the car and the smartphone are connected over the Internet and communicate to act–unlocking the door [56]. This function is often accomplished using a mobile application offered by the automobile manufacturer or a third-party app. However, this raises a concern about seaboutty issues,issues, such asone.

- Lightweight Security Solustions

  Smart cities are a big project requiring a huge investment in money, time, components, electricity, strong connection, and cloud computing [57]. In developing smart cities, concerns about data storage, limited resources, and battery life are essential to consider. For example, a smart door requires an unlimited battery life to allow users to open and close the door using their smartphone [58]. Taking blackout risk into consideration is also essential to ensure the smart door stays locked and can only be unlocked by the owner using an Offline Access Code.

- Authetication and Confidentially

  Said, authentication verifies a person's or a specific identification to ensure that the individual is whom they say they are [59], whereas confidentiality ensures that information is kept secret and protected from unauthorized access or exposure [60]. With the continuous growth of IoT development, authentication, and confidentiality is an essential aspects of every intelligent application. Many IoT terminal devices that make people's lives easier also give attackers a larger attack platform and environment [61]. An example of authentication that can be implemented is a password or passcode and face or fingertip identification in identifying the correct owner. End-

to-end encryption is an example feature that all apps should implement for confidentiality, which refers to keeping information private and preventing unauthorized access [62]. WhatsApp uses end-to-end encryption that keeps the user's private messages between the user and people they choose, not even WhatsApp can read or listen to them.

- Availability and Virtue

  In smart cities, availability refers to systems and resources that should be available and functioning when required [63], whereas integrity ensures that data is correct, up-to-date consistent, and secure against unauthorized access [64]. This is one of the challenges that smart cities encounter during their growth. Is the service always available, and is the data or information reliable? Employing blockchain technology can ensure data availability and integrity. Blockchain provides availability by distributing several copies of blockchain ledgers among nodes or computers; this redundancy ensures that even if specific nodes go offline or become unreachable, the Blockchain remains maintained and validated by other nodes in the network [65]. Procedures such as Proof of Work (PoW), which require a majority of network participants to agree on transaction validity, are how Blockchain helps maintain data integrity [66]. This consensus method improves the integrity of the data recorded in the Blockchain even further.

- Smart City Developments with Cloud/Fog Technology

  Fog-to-cloud computing is the foundation for smart city infrastructure, allowing for efficient data management, real-time processing, and intelligent decision-making [67]. While cloud computing is everyone’s go-to for data storage because of its high accessibility from anywhere and anytime, cloud computing may cause latency due to the need for data to be transmitted to and from the cloud servers [68]. Latency can impact the effectiveness of real-time processing data. Fog computing is introduced to mitigate this issue by processing data closer to the edge, reducing latency and enabling faster response times to overcome this problem [69]. In conclusion, fog computing helps extend cloud computing capabilities to the network's edge.

5. Recommendation

The embedded Secure Element (eSE) can transform the safeguarding of IoT connections in smart urban settings. It behaves like a chip that comes in any size and is made of secure operating systems and applications that can be embedded into any sort of device. It ensures that the data stored inside the chip is protected and that the information is only available for authorized access, and it also performs cryptographic activities such as authentication and encryption. In contrast to external secure components, which are separate chips or modules that may be added to a device, embedded secure elements are built into the device's architecture. The eSE is frequently embedded directly into the IoT device's microcontroller or system-on-chip (SoC), enabling a more streamlined and tightly integrated solution. These are several security and privacy benefits that can be achieved by integrating Secure Element (SE) into IoT devices.

- Secure Key Storage: Secure key storage is a secured section of flash controlled by and accessible only by SE. One example of an application that uses this feature is Google Sign-In Authentication. When a user tries to sign into their Google account on another device, Google will notify the user’s original device (first device signed in) and provide a token (numbers) for the user to insert on another device to allow sign-in.
- Secure Authentication: SE provides safe authentication procedures like hardware-based secure boot and secure key exchange, which improve the device's capacity to verify and establish trust with other parties in the IoT ecosystem.
- Immutable Device Identity: It is a unique and unchangeable identification assigned to an IoT device. It allows users to establish and validate the device's validity and integrity. Immutable device identification assures that device's identity cannot be tampered with or spoofed, which is essential for secure communication and trust establishment in IoT networks
- Data Protection: Permit the secure transfer and storage of sensitive data by implementing secure data encryption and decryption

- Secure Communication: IoT devices can use SE to establish encrypted and authenticated connections with other devices or cloud servers, protecting the confidentiality and integrity of data exchanged
- Privacy Preservation: To protect user privacy while enabling critical data analysis and insights, Secure Elements can offer techniques that protect privacy, such as safe multiparty computation or differential privacy

SmartCard by Thales is an example of a product that uses Secure Element Integration. Thales is the leading international provider of security solutions, including smart cards with embedded secure components. This SmartCard contains a CPU, memory, and applications. The rounded metal contact is essential for establishing an electrical connection with the chip beneath and initiating card functionality. It works with a contact or contactless card reader, which can be found in POS systems, ATMs, or mobile devices. SmartCard by Thales is a secure storage device for important details like secret keys, account numbers, passwords, or personal data. The advantage of this SmartCard is that it can effectively validate the PIN or fingerprint offline.

In conclusion, integrating secure elements in intelligent cities is critical for improving the Security and privacy of IoT connections. A solid and tamper-resistant hardware-based security foundation is formed by introducing secure element technology into IoT devices and systems. Smart Cities require advanced safety measures for efficient management and to meet regulatory requirements in many locations and specific sectors. In the never-ending arms race between hackers and device manufacturers, an integrated secure element provides tremendous value and cost savings to ensure device security. Compared to a specialized external SE, an integrated SE allows for significant cost savings. Using secure features in intelligent cities provides a future-proof solution that is resistant to evolving security risks and issues. It ensures that IoT devices and systems operate with greater integrity, laying the groundwork for safe data sharing, dependable authentication, and protection against security risks

6. Conclusion

Overall, the study of intelligent city architecture demonstrdigital-age urban infrastructure'ss digital-age urban infrastructure's. Sensors, networks, data platforms, and apps are just a few components that make intelligent city systems work. Analyzing smart city architecture reveals that a holistic and integrated strategy is required to ensure these cities' effective operation and management. Brilliant city theory must be implemented with the general consent of the people so thaso thathe country cacancatch up with other countries and not fall further behind. In the quest for a smart city, security issues must be addressed so that the city's reputation as a smart city is not jeopardized. Security and privacy concerns have grown in importance as intelligent gadgets have become more widely used, necessitating practical solutions. There are, of course, security and privacy concerns, but there are also solutions.

Acknowledgment

We sincerely thank the Computer Network course for its invaluable contribution to enriching our comprehension of IoT security and Blockchain. The acquisition of knowledge through the study of this subject has significantly influenced our understanding of these crucial areas and has equipped us with the necessary to explore and harness the potential of these technologies efficiently. We want to extend our heartfelt appreciation to our esteemed professors and educators for their steadfast dedication and diligent efforts in imparting invaluable knowledge to us. Their commitment has contributed significantly to our advancement in improving our skills and comprehension in the field of Computer Networking, IoT security, and Blockchain technology.

References

[1] W. S. de Amorim, A. Borchardt Deggau, G. do Livramento Gonçalves, S. da Silva Neiva, A. R. Prasath, and J. B. Salgueirinho Osório de Andrade Guerra, “Urban challenges and opportunities to promote sustainable food security through smart cities and the 4th industrial revolution,” *Land use policy*, vol. 87, p. 104065, Sep. 2019, doi: 10.1016/j.landusepol.2019.104065.

[2] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 650–655, Sep. 2018, doi: 10.1016/j.future.2018.04.060.

[3] T. Pratik, R. K. Lenka, G. K. Nayak, and A. Kumar, "An Architecture to Support Interoperability in IoT Devices," in *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Oct. 2018, pp. 705–710, doi: 10.1109/ICACCCN.2018.8748483.

[4] S. Misra, M. Reisslein, and G. Xue, "A survey of multimedia streaming in wireless sensor networks," *IEEE Commun. Surv. Tutorials*, vol. 10, no. 4, pp. 18–39, Dec. 2008, doi: 10.1109/SURV.2008.080404.

[5] K. Chopra, K. Gupta, and A. Lambora, "Future Internet: The Internet of Things-A Literature Review," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Feb. 2019, pp. 135–139, doi: 10.1109/COMITCon.2019.8862269.

[6] M. Alja'Afreh, "A QoE Model for Digital Twin Systems in the Era of the Tactile Internet," pp. 244, 2021. [Online]. Available at: https://ruor.uottawa.ca/handle/10393/42836%0A.

[7] F. Amalina *et al.*, "Blending Big Data Analytics: Review on Challenges and a Recent Study," *IEEE Access*, vol. 8, pp. 3629–3645, 2020, doi: 10.1109/ACCESS.2019.2923270.

[8] E. Benkhelifa, T. Welsh, and W. Hamouda, "A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3496–3509, 2018, doi: 10.1109/COMST.2018.2844742.

[9] W. Xing, R. Guo, E. Petakovic, and S. Goggins, "Participation-based student final performance prediction model through interpretable Genetic Programming: Integrating learning analytics, educational data mining and theory," *Comput. Human Behav.*, vol. 47, pp. 168–181, Jun. 2015, doi: 10.1016/j.chb.2014.09.034.

[10] R. Amin, R. S. Sherratt, D. Giri, S. H. Islam, and M. K. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," *IEEE Trans. Consum. Electron.*, vol. 63, no. 1, pp. 53–61, Feb. 2017, doi: 10.1109/TCE.2017.014735.

[11] S. Pirbhulal, V. Gkioulos, and S. Katsikas, "A Systematic Literature Review on RAMS analysis for critical infrastructures protection," *Int. J. Crit. Infrastruct. Prot.*, vol. 33, p. 100427, Jun. 2021, doi: 10.1016/j.ijcip.2021.100427.

[12] I. V. Lokshina, M. Greguš, and W. L. Thomas, "Application of Integrated Building Information Modeling, IoT and Blockchain Technologies in System Design of a Smart Building," *Procedia Comput. Sci.*, vol. 160, pp. 497–502, Jan. 2019, doi: 10.1016/j.procs.2019.11.058.

[13] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Comput. Sci. Rev.*, vol. 38, p. 100312, Nov. 2020, doi: 10.1016/j.cosrev.2020.100312.

[14] T. M. Ghazal *et al.*, "IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare—A Review," *Futur. Internet*, vol. 13, no. 8, p. 218, Aug. 2021, doi: 10.3390/fi13080218.

[15] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1025–1035, Dec. 2016, doi: 10.1109/JIOT.2016.2547994.

[16] F. Irram, M. Ali, M. Naeem, and S. Mumtaz, "Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions," *J. Netw. Comput. Appl.*, vol. 206, p. 103431, Oct. 2022, doi: 10.1016/j.jnca.2022.103431.

[17] A. Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Secure IoT Structural Design for Smart Homes," in *Smart Cities Cybersecurity and Privacy*, Elsevier, 2019, pp. 187–201, doi: 10.1016/B978-0-12-815032-0.00013-5.

[18] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain," *J. Inf. Secur. Appl.*, vol. 45, pp. 156–175, Apr. 2019, doi: 10.1016/j.jisa.2019.02.003.

[19] N. P. Owoh and M. M. Singh, "Security analysis of mobile crowd sensing applications," *Appl. Comput. Informatics*, vol. 18, no. 1/2, pp. 2–21, Mar. 2022, doi: 10.1016/j.aci.2018.10.002.

[20] A. Cuzzocrea and E. Damiani, "Privacy-Preserving Big Data Exchange: Models, Issues, Future Research Directions," in *2021 IEEE International Conference on Big Data (Big Data)*, Dec. 2021, pp. 5081–5084, doi: 10.1109/BigData52589.2021.9671686.

[21] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for Internet of Things-based Energy Internet," *Futur. Gener. Comput. Syst.*, vol. 93, pp. 849–859, Apr. 2019, doi: 10.1016/j.future.2018.01.029.

[22] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart Transportation: An Overview of Technologies and Applications," *Sensors*, vol. 23, no. 8, p. 3880, Apr. 2023, doi: 10.3390/s23083880.

[23] S. Vappangi and V. V. Mani, "Concurrent illumination and communication: A survey on Visible Light Communication," *Phys. Commun.*, vol. 33, pp. 90–114, Apr. 2019, doi: 10.1016/j.phycom.2018.12.017.

[24] Y. Pan and L. Zhang, "Roles of artificial intelligence in construction engineering and management: A critical review and future trends," *Autom. Constr.*, vol. 122, p. 103517, Feb. 2021, doi: 10.1016/j.autcon.2020.103517.

[25] R. Bibi *et al.*, "Edge AI-Based Automated Detection and Classification of Road Anomalies in VANET Using Deep Learning," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–16, Sep. 2021, doi: 10.1155/2021/6262194.

[26] H. (Harrison) Jeong, Y. (Chris) Shen, J. (Paul) Jeong, and T. (Tom) Oh, "A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications," *Veh. Commun.*, vol. 31, p. 100349, Oct. 2021, doi: 10.1016/j.vehcom.2021.100349.

[27] A. Pramono and T. I. W. Primadani, "Smart home apps for saving energy usage at griyapram guesthouse malang," in *AIP Conference Proceedings*, Apr. 2023, vol. 2594, no. 1, p. 060008, doi: 10.1063/5.0109445.

[28] W. Li, T. Yigitcanlar, I. Erol, and A. Liu, "Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework," *Energy Res. Soc. Sci.*, vol. 80, p. 102211, Oct. 2021, doi: 10.1016/j.erss.2021.102211.

[29] R. Pastorino *et al.*, "Benefits and challenges of Big Data in healthcare: an overview of the European initiatives," *Eur. J. Public Health*, vol. 29, no. Supplement_3, pp. 23–27, Oct. 2019, doi: 10.1093/eurpub/ckz168.

[30] C. Chen, Y. Hu, M. Karuppiah, and P. M. Kumar, "Artificial intelligence on economic evaluation of energy efficiency and renewable energy technologies," *Sustain. Energy Technol. Assessments*, vol. 47, p. 101358, Oct. 2021, doi: 10.1016/j.seta.2021.101358.

[31] A. AlDairi and L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," *Procedia Comput. Sci.*, vol. 109, pp. 1086–1091, Jan. 2017, doi: 10.1016/j.procs.2017.05.391.

[32] M. H. Panahi Rizi and S. A. Hosseini Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," *Internet of Things*, vol. 20, p. 100584, Nov. 2022, doi: 10.1016/j.iot.2022.100584.

[33] M. K. Hasan *et al.*, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Commun.*, vol. 16, no. 5, pp. 421–432, Mar. 2022, doi: 10.1049/cmu2.12301.

[34] Z. A. Baig *et al.*, "Future challenges for smart cities: Cyber-security and digital forensics," *Digit. Investig.*, vol. 22, pp. 3–13, Sep. 2017, doi: 10.1016/j.diin.2017.06.015.

[35] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions," *Wirel. Networks*, vol. 27, no. 1, pp. 55–90, Jan. 2021, doi: 10.1007/s11276-020-02445-6.

[36] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and*

Systems (HPCC/SmartCity/DSS), Dec. 2016, pp. 1392–1393, doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[37] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.

[38] L. Zhou, C. Su, W. Chiu, and K.-H. Yeh, "You Think, Therefore You Are: Transparent Authentication System with Brainwave-Oriented Bio-Features for IoT Networks," *IEEE Trans. Emerg. Top. Comput.*, vol. 8, no. 2, pp. 303–312, Apr. 2020, doi: 10.1109/TETC.2017.2759306.

[39] R. Amin, R. S. Sherratt, D. Giri, S. H. Islam, and M. K. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," *IEEE Trans. Consum. Electron.*, vol. 63, no. 1, pp. 53–61, Feb. 2017, doi: 10.1109/TCE.2017.014735.

[40] Y. Wang, J. Wan, J. Guo, Y.-M. Cheung, and P. C. Yuen, "Inference-Based Similarity Search in Randomized Montgomery Domains for Privacy-Preserving Biometric Identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 7, pp. 1611–1624, Jul. 2018, doi: 10.1109/TPAMI.2017.2727048.

[41] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, "Data Mining for Internet of Things: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 77–97, 2014, doi: 10.1109/SURV.2013.103013.00206.

[42] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1025–1035, Dec. 2016, doi: 10.1109/JIOT.2016.2547994.

[43] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in Location Based Services," in *2013 Proceedings IEEE INFOCOM*, Apr. 2013, pp. 2985–2993, doi: 10.1109/INFCOM.2013.6567110.

[44] Lei Xu, Chunxiao Jiang, Yan Chen, Yong Ren, and K. J. R. Liu, "Privacy or Utility in Data Collection? A Contract Theoretic Approach," *IEEE J. Sel. Top. Signal Process.*, vol. 9, no. 7, pp. 1256–1269, Oct. 2015, doi: 10.1109/JSTSP.2015.2425798.

[45] N. Walravens, "Mobile Business and the Smart City: Developing a Business Model Framework to Include Public Design Parameters for Mobile City Services," *J. Theor. Appl. Electron. Commer. Res.*, vol. 7, no. 3, pp. 21–22, 2012, doi: 10.4067/S0718-18762012000300011.

[46] M. Batty *et al.*, "Smart cities of the future," *Eur. Phys. J. Spec. Top.*, vol. 214, no. 1, pp. 481–518, Nov. 2012, doi: 10.1140/epjst/e2012-01703-3.

[47] N. Aleisa and K. Renaud, "Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, 2017, pp. 198–205, doi: 10.5220/0006233701980205.

[48] M. U. Younus, S. ul Islam, I. Ali, S. Khan, and M. K. Khan, "A survey on software defined networking enabled smart buildings: Architecture, challenges and use cases," *J. Netw. Comput. Appl.*, vol. 137, pp. 62–77, Jul. 2019, doi: 10.1016/j.jnca.2019.04.002.

[49] N. Azzaoui, A. Korichi, B. Brik, M. el amine Fekair, and C. A. Kerrache, "Wireless communication in internet of vehicles networks," in *Proceedings of the 4th International Conference on Smart City Applications*, Oct. 2019, pp. 1–6, doi: 10.1145/3368756.3368998.

[50] F. Touati, A. Ben Mnaouer, O. Erdene-Ochir, W. Mehmood, A. Hassan, and B. Gaabab, "Feasibility and performance evaluation of a 6LoWPAN-enabled platform for ubiquitous healthcare monitoring," *Wirel. Commun. Mob. Comput.*, vol. 16, no. 10, pp. 1271–1281, Jul. 2016, doi: 10.1002/wcm.2601.

[51] T. Monahan and J. T. Mokos, "Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks," *Geoforum*, vol. 49, pp. 279–288, Oct. 2013, doi: 10.1016/j.geoforum.2013.02.001.

[52] S. Shah, C. B. Soriano, and A. D. Coutroubis, "Is big data for everyone? the challenges of big data adoption in SMEs," in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Dec. 2017, vol. 2017-Decem, pp. 803–807, doi: 10.1109/IEEM.2017.8290002.

[53] I. Rubinstein, "Big Data: The End of Privacy or a New Beginning?," *SSRN Electron. J.*, pp. 12-56, Oct. 2012, doi: 10.2139/ssrn.2157659.

[54] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Comput. Commun.*, vol. 54, pp. 1–31, Dec. 2014, doi: 10.1016/j.comcom.2014.09.008.

[55] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018, doi: 10.1109/JIOT.2017.2767291.

[56] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart Locks," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, May 2016, pp. 461–472, doi: 10.1145/2897845.2897886.

[57] M. Lom and O. Pribyl, "Smart city model based on systems theory," *Int. J. Inf. Manage.*, vol. 56, p. 102092, Feb. 2021, doi: 10.1016/j.ijinfomgt.2020.102092.

[58] I. Chatzigiannakis, "Apps for smart buildings," in *Start-Up Creation*, Elsevier, 2016, pp. 465–479, doi: 10.1016/B978-0-08-100546-0.00019-4.

[59] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," *IEEE Secur. Priv.*, vol. 1, no. 2, pp. 33–42, Mar. 2003, doi: 10.1109/MSECP.2003.1193209.

[60] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," *Secur. Priv.*, vol. 1, no. 2, p. e20, Mar. 2018, doi: 10.1002/spy2.20.

[61] Y. Lu and L. Da Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019, doi: 10.1109/JIOT.2018.2869847.

[62] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[63] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, Mar. 2012, doi: 10.1016/j.future.2010.12.006.

[64] G. Sivathanu, C. P. Wright, and E. Zadok, "Ensuring data integrity in storage," in *Proceedings of the 2005 ACM workshop on Storage security and survivability*, Nov. 2005, pp. 26–36, doi: 10.1145/1103780.1103784.

[65] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019, doi: 10.1109/COMST.2019.2894727.

[66] N. A. Akbar, A. Muneer, N. ElHakim, and S. M. Fati, "Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses," *Futur. Internet*, vol. 13, no. 11, p. 285, Nov. 2021, doi: 10.3390/fi13110285.

[67] C. Zhang, "Design and application of fog computing and Internet of Things service platform for smart city," *Futur. Gener. Comput. Syst.*, vol. 112, pp. 630–640, Nov. 2020, doi: 10.1016/j.future.2020.06.016.

[68] W. Shi and S. Dustdar, "The Promise of Edge Computing," *Computer (Long. Beach. Calif).*, vol. 49, no. 5, pp. 78–81, May 2016, doi: 10.1109/MC.2016.145.

[69] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for Healthcare 4.0 environment: Opportunities and challenges," *Comput. Electr. Eng.*, vol. 72, pp. 1–13, Nov. 2018, doi: 10.1016/j.compeleceng.2018.08.015.