ISSN 2614-0047

Empowering smart city governance through decentralized blockchain solutions for security and privacy in IoT communications

Ahmad Anwar Zainuddin [a,1,*], Nurul Fadhilah Ahmad Muhammad [a], Amir Husaini Mohd Hasli [b], Nor Ani Jannah Ahmad Zaini [b], Nureen Batrisyia Balqis Karimudin [a], Hannah Sabrina Saiful Bahri[a], Muhamad Khaleesh Mirza Khairul Nizam [c], Saidatul Izyanie Kamarudin [d], Nasyitah Ghazalli [e]

[a] Department of Computer Science, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia
[b] Department of Information System, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia
[c] Kolej Kemahiran Tinggi MARA Petaling Jaya, Malaysia
[d] College of Computing, Informatics and Media University Technology MARA (UiTM), Malaysia
[e] Research and Technology, Thales, United Kingdom
[1] mr.anwarzain@gmail.com
* corresponding author

ARTICLE INFO

Article history
Received July 29, 2023
Revised August 18, 2023
Accepted November 4, 2023

Keywords
Smart city
Urban issues
Security
Privacy

ABSTRACT

This paper highlights the benefits and challenges of smart cities, which leverage technology to offer a wide range of services to citizens. While these services have the potential to greatly improve the quality of life in metropolitan areas, they also raise significant privacy and security concerns. The study emphasizes the need to employ "privacy by design" principles to ensure that personal data is protected throughout the entire lifecycle of data, and data owners have the self-control to manage their data according to their preferences. Smart contracts, built on blockchain technology, offer a secure and transparent way of conducting transactions, particularly in e-governance, and automating processes. By leveraging these technologies, smart cities can address the privacy and security challenges they face while continuing to offer cutting-edge services to their inhabitants. Ultimately, the study emphasizes the importance of a proactive approach to privacy and security in the development and implementation of smart cities.

1. Introduction

The United Nations (UN) estimated that by the year 2050, 70% of the world's population would be living in cities [1]. Due to the increasing number of those living in urban areas, energy consumption would also increase causing many environmental related issues. One of the ideas to combat this issue is by using technological infrastructures such as Smart Cities. Smart Cities in general consist of the use of information and communication technology (ICT) which includes the Internet of Things (IoT). It is a technology-based infrastructure that provides numerous solutions to standard problems. Artificial Intelligence (AI) is the example of IoT based technology. AI helps in maintaining a sustainable and responsive city which includes analysing how a city consumes energy, waste management, and transportation usage.

Based on the Smart Nation program in 2014, Singapore takes the throne to be one of the countries that have successfully developed the use of IoT in its cities [2]. The creation of the National Digital Identity, contactless payments, the utilisation of environmentally friendly energy sources, and the

introduction of autonomous buses and shuttles are just a few instances of how the programme was put into practise. The digital health system is one of the interesting technologies that has been created to alleviate the strain of an ageing population where they also deployed wearable Internet of Things devices in order to monitor the health of patients.

The idea of Smart Cities indeed has incredible perks towards everyone's lives, by making it easier and more sustainable, but it also has its drawbacks. Because of Smart Cities being an IoT infrastructure, it is vulnerable towards cyber-attacks. This may include the invasion of privacy and personal data breach. Fig. 1 indicates the IoT security and privacy concern. Despite its rapid growth, IoT still faces security and privacy concerns. Several companies are now assisting businesses in using IoT to solve long-standing, industry-specific challenges. They create Internet of Things (IoT) solutions that connect things, collect data, and derive insights using open and scalable solutions that reduce costs, improve productivity, and increase revenue [3]. The rapid evolution of communication technologies, particularly in IoT, implies that the potential challenges go beyond technical aspects, such as data protection and privacy. As a result, the growth of IoT opens a wide range of opportunities.

Based on a case study, America has developed a new surveillance technology known as PRISM and XKeyscore, a program designed to detect any dangerous terrorist attacks. The U.S. government was able to access people's Google, Yahoo, Apple, Microsoft accounts thanks to PRISM whereas emails, website traffic, and other types of global Internet data were gathered and analysed by Xkeyscore [4].

This article is presented in the following manner. Section 2, describes the literature overview of this paper; section 3 discussed the architecture of smart cities and its applications Section 4 describes secure architecture using Black Networks (BN), Trusted Software-Defined Networks (SDN) Controllers Trusted Software-Defined Networks (SDN) Controllers and Unified registry; section 5 analyse the open issues and future research direction; section 6 discussed methods on how to improved security and privacy in IoT communication in smart cities; Section 7 concludes the concept of implementation security in smart cities as well as sustainable and user-friendly architecture

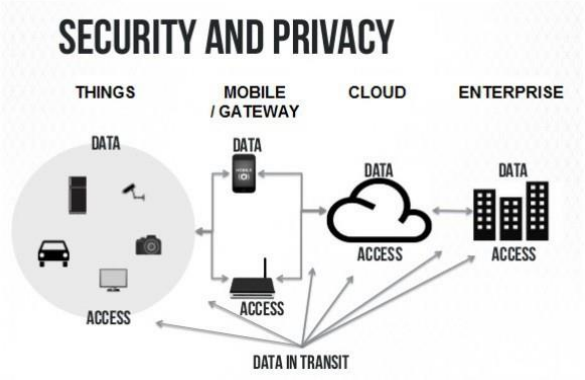

Fig. 1. IoT security and privacy concern

2. Literature Overview

The literature review in this research can be seen in Table 1.

Table.1 Literature Overview

Article	Key findings / Arguments	Supporting Evidence / Sample Characteristics / Methods	Strengths / Limitations	Significance / Implications
Research Question: Security and privacy in IoT communications in smart cities				
[5]	One of the key tenets of the coming digital era to better the lives of humans is the idea of the smart city.	Modern technological advancements are digitising existing	The process of continuously evaluating the security of IoT	In order to provide trustworthy smart cities for the benefit of society, these issues

Article	Key findings / Arguments	Supporting Evidence / Sample Characteristics / Methods	Strengths / Limitations	Significance / Implications
		urban areas to offer data-driven services.	devices can be improved using automated security measures.	will necessitate an adaptation of present technical and legislative solutions. New emerging technologies, such as 5G, blockchain, and AI techniques, will be developed.
[6]	Building a smart city to provide numerous valuable time and resource-saving advantages demands higher levels of network connectivity to support new advanced features, which raises issues about security and privacy.	The Internet of Things (IoT) devices currently in use, which oversee gathering data from various sources and transferring it to storage facilities through the existing networks, increase the attack surface and could serve as a point of entry for malicious attackers looking to compromise the system.	The cities also have several widespread video surveillance systems and GPS for gathering very sensitive data, which might be exploited by attackers to track down residents and seriously jeopardise their privacy.	In order to lower the quality of intelligent services in smart cities, the malicious node and devices can execute a variety of assaults, including denial-of-service, eavesdropping, SQL injection, session hijacking, and brute-force attacks. .
[7]	The importance of acquiring a secure IoT architecture in Smart Cities that is free of vulnerabilities in order to provide a safe and private communication system.	A secure architecture that consists of Black Networks, Trusted SDN Controller, Unified Registry and Key Management System that increases and aids the baseline security that is already provided.	A detailed explanation on the IoT security architecture as well as providing real life examples that shed light on the topic.	The importance of the four components in the IoT's architectural platform to combat malicious threats and create a safe space for technology to advance.
[8]	Researchers have a keen interest in data security and privacy in smart cities. In a smart city, the security depends on three different issues: those relating to government, those pertaining to the socioeconomic sector, and finally, technology perspectives	From a social perspective, issues with communication, citizen safety, travel, banking, and finance are all important. Utility, health, infrastructure, education, and transportation are governance concerns. Technical issues include RIFD, smart grid, biometrics, M2M	The graphical and mathematical model helps with the Internet of Things by locating servers, people, and security and privacy concerns, but the methodology is not covered	IoT is important for creating smart cities, thus distributed framework can effectively address difficulties with information security in these cities to a big extent

Article	Key findings / Arguments	Supporting Evidence / Sample Characteristics / Methods	Strengths / Limitations	Significance / Implications
		connectivity, and smart phones		
[5]	An IoT-enabled smart city generates data that is transferred to cloud servers for subsequent processing. By finding patterns in vast amounts of data and creating automated decision-making procedures, high-level services can be rendered	To balance the interests of citizens for privacy, differential privacy approaches must be used in conjunction with cryptographic techniques like secure multiparty computation and homomorphic encryption.	As firms can monetize individuals' data by allowing third parties to handle this information, data analytics techniques may have social, legal, and ethical implications	To ensure that GDPR and other legal requirements are met in IoT-enabled smart cities, the use of techniques like pseudonymization, encryption, aggregation, or data usage management must be considered
[9]	Due to its strong realistic demand and practical backdrop in an increasingly urbanised world, the notion of the "smart city" has garnered increasing attention in both academic and industrial disciplines over the past two decades	An increasing number of cities around the world have started to build their own smart strategies to address these issues, enhance citizen well-being, spur economic growth, and administer contemporary cities in a sustainable and intelligent manner	Due to the weaknesses that are frequently present at each layer of a smart system, the development of these smart applications could, nevertheless, result in significant security and privacy issues. Attacks like Sybil, denial of service (DoS), and illegal access can reduce the quality of intelligent services	Additionally, citizens face privacy issues as a result of service providers and some third parties collecting too much data
[10]	The use of MCS is expanding in the modernization period because of its capability of sensing people's surroundings and retrieving helpful real-time information.	The presence of available mobile applications that have a high sense of detection of a mobile device's surrounding	Although MCS is an interesting and fast technique in collecting data, it also comes with its drawbacks and challenges	MCS is useful for gathering authentic data in order to devise a solution to a problem
[7]	The widespread use of Internet of Thing in smart cities greatly expands the attack that happen to the system in the smart city by making every IoT devices and their communications a possible entry point to the system	Multiple attack of ransomware on companies, cities and local governments have been initiated. Even cities become extremely prone as a result of smart technologies and widespread automation	All the cyber-security assaults provide a complex danger to IoT network. Building a secure IoT-based smart city involves a different approach to the security and smart system infrastructure	Artificial Intelligence are employed at different levels to enable adaptation in the local system as well as to monitor the system's health and security in order to evaluate, acquire and store the big data that produced in the cloud

3. Method

3.1. Architecture Of Smart Cities

There are several architectures that have been developed to match with the development of smart cities. Nevertheless, from the survey, the study will introduce an Internet of Things (IoT) based architecture that puts a significant focus on the problems regarding privacy and security in smart cities. Fig. 2 illustrates the architecture of smart city, and the following subsections give a concise explanation of each layer of the architecture.

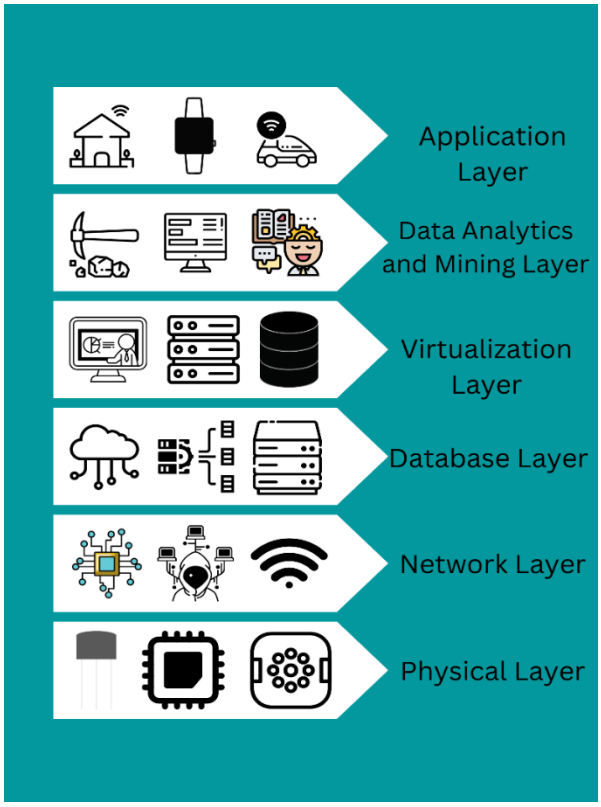

Fig. 2. The layer of architecture of smart cities

- Physical Layer

  The OSI Model's Physical layer is its base layer. This layer specifies how a device and a transmission medium link. Based on the figure above, it is equipped with several sensors and actuators that collect data and transmit it to the architecture's network layer for further processing.

- Network Layer

  Meanwhile, the network layer is at the third layer of the OSI Model. It responds to incoming requests from the transport layer and passes them on to the data link layer. The network layer is the central layer of the IoT architecture; thus, it depends on basic networks including the Internet, Wireless Sensor Networks (WSNs) and communication networks [11]. The key role of the network layer is to transmit data that have been collected by the physical layer and connecting servers and other network devices.

- Database Layer

  The database layer complies with the architecture's upper layers. It involved intelligent computer systems and database servers. This layer's primary function is to fulfil application needs using the latest computing techniques like cloud computing.

- Virtualization Layer

  This layer offers a virtual network integration technique that combines network capabilities with hardware or software into a single software-based layer, logically configurable entity. Platform

and resource virtualization may be necessary for a network virtualization to be successful. It will be achieved by utilizing the virtualization layer.

- Data Analytics and Mining Layer

  Next, in this layer raw data is processed into a useful knowledge that helps the network to run more efficiently and detects future occurrences like system failure. To examine the data, the data analytics and mining layer uses several data mining and analytics approaches including machine learning algorithms [11].

- Application Layer

  The application layer comes last. Application layer is located at OSI Model's seventh layer, which is its topmost layer. For this layer, it offers citizens smart and intelligent services and applications tailored to their individual requirements. The following questions will go over more details about the application layer.

3.2. Application of Smart Cities

There are numerous applications that make use of information technology and technological advancements as depicted in Fig. 3. These applications are useful to handle urban concerns and raise living standards, promote economic development, sustain environmental quality, and administer cities in a more effective and secure manner. The use of the internet via smart devices can conveniently connect useful applications that make life simpler for people and save time. For example, the use of the internet for environment, transportation, buildings, and healthcare. The next part is some of the examples of the applications that we are highlighted.

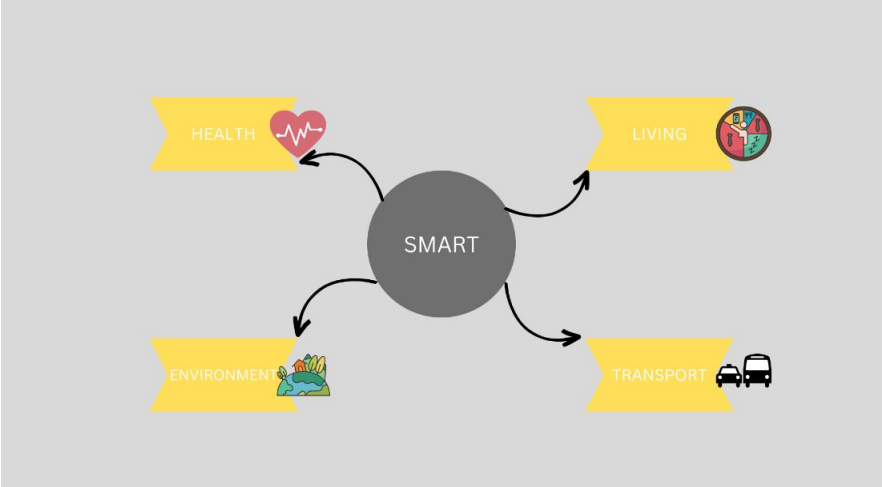

Fig. 3. Application of smart cities in daily lives

- Smart Health

  The idea behind smart health in smart cities is to deliver healthcare service via networks and from the sensor within the infrastructure of smart cities. For instance, by constantly monitoring real-time data to detect infectious diseases such as influenza, common cold, chickenpox and so on at an early stage, smart healthcare applications strive to enhance the quality of the existing healthcare system. Additionally smart health provides remote consultation and medical surveillance functions for those who are suffering with chronic illness. Some applications use cloud services to access analysed health data. This include electrocardiogram (ECG) and electrical impedance tomography (EIT) signals that is obtained from wearables and other sensor devices such as health watch which is also known as fitness smart watch.

- Smart Living

  Smart living enables intelligent control over numerous utilities and equipment in the houses to simultaneously create comfortable spaces and optimize energy efficiency. It also enables surveillance, entertainment, education and climate control. Furthermore, smart living applications a intelligently control waste recycling, social networking, parking in the neighbourhood or building to give the residents of the smart neighbourhood live comfortably, individual needs services and a sustainable environment [11].

- Smart Transportation

  One of the key research areas for smart transportation is navigation and route optimization. The optimization on route planning is studied to evaluate traffic congestion and thus, provide the best route options to shorten commute times. As a result, it will reduce car emissions and minimize carbon footprint. These applications use data from the users' mobile devices or using side units installed in specific spots on the road [12]. For example, traffic lights that are equipped with closed-circuit television (CCTV). If there is an accident near this CCTV, an alert will be sent immediately to the rescuers such as police or firefighters. Traffic lights can also work according to the importance of looking at the section with more vehicles and not according to the set time. This can save time and energy consumption. Other than that, using cameras and IoT devices, smart parking systems have been developed. The system will detect any empty parking spaces and will guide the user to that place.

- Smart Environment

  Smart environment is related to the things around us. The problem that peoples face in relation to the environment is high electricity bills. Therefore, with the presence of connected and integrated LED lighting systems with motion sensor, can minimize the use of electricity because this light can autonomously dim or turn off rooms or other spaces when unoccupied.. In addition, the application of weather sensors can manage automatic watering system and detect leaks. Moreover, smart sensors can monitor the air quality and water pollution levels across the city and river level to prevent floods.

3.3. Citie's Applications

Currently, the issue of smart city development is attracting an attention among industry and research communities. This is because every country is racing to follow this smart city trend. Consequently, every nation will work hard to progress its technology in order to realise its vision of becoming a smart city. Everything has pros and cons. In line with the progress of this smart city, there are also security and privacy issues that have arisen which are the main obstacles in the effort to make a smart city. We need to be careful in dealing with this issue. Therefore, we outline and briefly examine some of the key components of this security challenge in the following sections.

3.3.1. Cyber Security

What is the meaning of cyberattacks? Cyberattacks is any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. Most victims of this cyberattack are not aware of the attack. This is because some cyberattacks are carried out silently and users are not aware of it. For example, in browser attack, when a user opens a website, the attacker exploits the vulnerabilities in the browser of the website and eventually obtains user's information. There are two types of attacks: active and passive. A passive attack means that the attack is only to steal data and the hacker does not change the data and information while an active attack is when the hacker changes the existing data. Therefore, there are several examples of (Fig. 4) cyberattacks affecting the security of smart city applications. among them are :

- Malware

  This harmful software has the potential to access the system unauthorizedly. To steal, alter, and destroy physical system components and related information, it can also take advantage of inherent holes in the system. Smart cities, for instance, might have several closed-circuit television cameras that are managed either privately or by public agencies. It is difficult to maintain the security of these cameras because some of them lack encryption methods and others are susceptible to virus assault. Accessing a camera can give one a means to look inside people's houses or utilise a bank camera to monitor and manage the users' keystrokes.

- Eavesdropping

  This is an instance of a passive attack, which is defined as unlawfully listening to communication without consent. Eavesdropping is a risky attack in smart cities that compromises network confidentiality and integrity and can result in failures on the personal and financial fronts. It can also be used to monitor communication channels to record the behaviour of network traffic and get the network map.

- Masquerading

  It is also referred to as "identity spoofing" or "impersonation." By posing as a legitimate object or entity, the attacker attempts to steal information through masquerading. For instance, masquerading can give unwanted access to confidential information in the intelligent transport system (ITS), a smart city application. This could compromise the network's integrity. Information in ITS may potentially be lost, corrupted, or altered as a result.

- False information (FI)

  Attackers send an incorrect quantity of FI via the network, which may have an impact on how other drivers behave. Both purposeful and inadvertent behavior is possible. As individuals act based on the FI provided to them, introducing FI to the systems in smart cities may cause delays and unneeded congestion.

- Message modification

  In this attack, the message is changed to cause the system to behave unexpectedly. Rearranging a message stream and/or delaying a message are both examples of message modification. Similar to FI, message alteration can affect data integrity by causing unneeded system delays and congestion. As a result, a threat to data integrity may affect residents and smart city infrastructure.

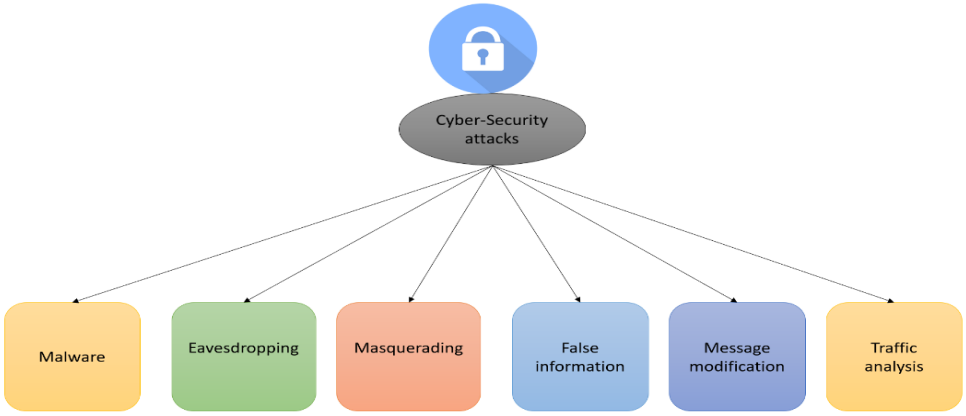

Fig. 4. Summary of the cybersecurity attacks in smart cities

- Traffic analysis (TA)

  Similar to eavesdropping, traffic analysis involves monitoring traffic patterns in order to gather information that can be used against the attackers. Eavesdropping and TA together could compromise privacy. The confidentiality of information in smart cities can also be harmed by unlawful information being obtained through TA assaults.

3.3.2. Botnet

Mirai is one of the IoT bot malware. Malware is software created with the purpose of interfering with, harming, or allowing unauthorised access to a computer system. Before it impacts a lot of computers, malware needs to be found. Malware scans through ranges of IP addresses looking for devices to attack, and once an IP have been found, a set of default credentials is used in order to log in and take control over the device [13]. Mirai attacks routers and cameras. The effect of botnet is to make high internet bills, unstable computer performance, potential legal implications if computer is compromised and stolen personal data in blackmail or identity theft. Bots scan addresses over a permitted range of IP addresses that set up to the local network, via the Internet.

3.3.3. Privacy Leakage

Hackers have the capability to collect, transmit, and process confidential material, including lifestyle data gleaned from intelligent surveillance systems, user identities and locations in the context of transportation, and health issues. This thus exposes the smart cities to privacy leaks. To fix this problem, a variety of security and privacy techniques (such as anonymity, access control, and encryption) can be used to protect sensitive data in smart cities against hacker attacks. However, most

of the security and privacy techniques currently in use are mainly intended to prevent external attackers and do not take possible inside attackers into consideration. For example, if the organization want to spot robberies or any odd activity, they use a camera as CCTV at the building. However, there is a possibility that the employees who have access to surveillance recordings could steal sensitive information or open a door for outside attackers. It is so challenging to develop a security and privacy system for smart cities that achieves a balance between privacy and effectiveness.

3.4. Security and Privacy Solutions for Smart Citie's Environment

This section introduces several security and privacy solutions that are used to overcome with possible threats to security and privacy in smart environments as shown in Fig. 5.

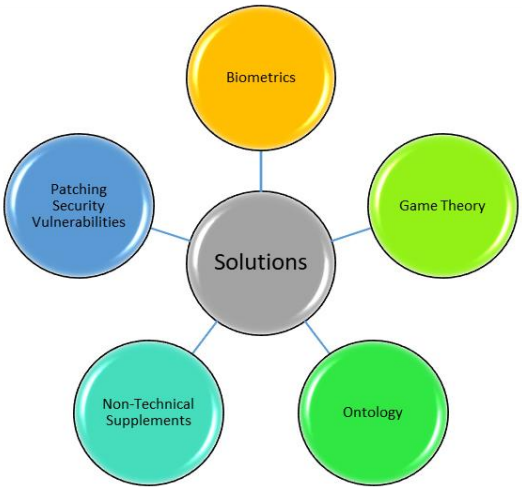

Fig. 5. Security and Privacy solutions for smart city

- Biometrics

  Biometrics are commonly used for validation in IoT-based systems. This automation may be applied to automatically detect a human based on biological traits and unique behavioural. Biodata is derived from faces, fingerprint, handwritten signatures, voices, and other biometrics. Brainwave-based authentication is one way worth noting here since it can achieve high authentication accuracy while also ensuring efficiency [14]. Amin et al. suggested a mutual authentication and key negotiation system to secure users' sensitive information in storage devices [15]. In compared to existing analogous systems, the unique protocol effectively resists security assaults and maintains communication overhead and cost. Another feature to consider is if these bio-based approaches are not employed correctly, the probability of privacy leaking will develop. It was suggested by Natguanathan et al. [16] to construct privacy-preserving biometric systems (PPBSs) which supported by the study done by Wang et al., [17]. This study also predicted a bright future for biometrics in different areas, for example e-commerce.

- Game Theory

  A strong mathematical instrument, game theory effectively employed in the disciplines of privacy protection and cybersecurity, based on the variety of application scenarios [18]. Do et al. [19] performed a comprehensive study that documented the characteristics of the game-theoretical method and its benefits over traditional defence mechanism such as timely action, distributed solutions, proven mathematics, reliable defence. Accordingly, there has been a surge in interest in utilising game theory to solve security and privacy challenges in applications based on IoT in recently. Abass et al. [20], for example, used evolutionary game theory to design unique attack analysis algorithms for cloud storage. Sedjelmaci et al. [21] focused on weak devices and suggested a lightweight anomaly detection approach that assures accuracy while consuming less energy. La et al. [22] developed a theoretical game model to explore the problem in deceptive attack and defence game in honeypot-enable networks, with a focus on communication security challenges in networks. The concept is adaptable to a newly developing IoT applications such as smart buildings, sensor networks, and smart healthcare. Wang et al. [23] presented a honeypot game to solve attack vulnerabilities in networks infrastructure with advanced metering in recent research. Xiao et al., [24] in another study, found that spoofing attack can be identify in wireless

networks by using a zero-sum game. In terms of privacy, numerous research combines game theory with other privacy protection technologies, such as k-anonymity [25] and differential privacy [26], to create mechanisms. Furthermore, Xu et al. [27] agree that game theory is a useful tool for balancing protection intensity and data value. Although fewer studies have applied game theory to a specific smart city application, many technologies have been developed within the scope of IoT security, and we believe that with the rapid evolution of everything-connected smart cities, game-theoretic approaches will play a significant role in solving some new security and privacy issues of this smart era

- Ontology

  One of the major branches of philosophy, ontology, has been identified as a promising tool for dealing with heterogeneous issues, particularly for unstructured data, knowledge, and configurable systems. The primary goal of using ontology is to better understand, describe, and reuse formally represented knowledge, as well as to search for new knowledge and isolate inconsistencies. Many ontology-based efforts to solve security and privacy problems, such as cyber-attack detection and security management, have advanced due to the inherent features. However, the application of ontology to the IoT domain is a new area, with only a few related efforts in recent years. Tao et al. [28] created a novel ontology-based security management model for smart homes that allows smart devices to interact more effectively while also improving system security. Mohsin et al. [29] proposed an ontology-driven security analysis framework for smart homes to support automatically capturing consistencies during interactions. Kim et al. [30] developed an ontology-based model called QoPI to characterise, represent, and manage users' personalised and dynamic privacy-control patterns in mobile computing situations, as previously stated. Lee et al. [31] provided a novel definition of "trust ontology" and used it to measure trustworthiness among content providers and consumers based on user preferences, purposes, and perspectives. One obvious limitation of current ontology-based studies in IoT security is that most of them focus on a specific application scenario or requirement and lack of a unified model, which reduces the value of their application. To address this issue, Xu et al. [32] proposed a semantic-ontology-based situation reasoning method in 2017 that provides a more comprehensive view of the security situation while also improving emergency response capability. Unfortunately, this method only addresses the network layer of IoT architecture and does not address overall security issues.

- Non-Technical Supplements

  Protection cannot be achieved solely by technical solutions. Existing technological limitations can be mitigated by strengthening related policies, regulations, governance, education and so on. Sound governance is critical to developing a dependable smart system from the standpoint of governance and politics. Walravens [33] stated that it is the obligation of the government to delicately study whether who has access to the data and what type of data may be assess. At the same time, Batty et al. [34] stated that law applied by the government must protect the model development and the data in a smart city framework. It is also crucial to give manufacturers, service providers, and users with training aimed at enhancing their relevant abilities. For instance, training should enable application designers to create solid and durable coding. Vendors oversee patching flaws in firewall software. Additionally, equipment manufacturers ought to do everything within their power to raise the general bar for safety and quality. The goal of education programmes is to increase awareness and understanding of citizens in how smart applications work and how to stay safe. Effectiveness is still a problem. Aleisa and Renaud [35] discovered that even while some users are aware of the possible dangers of privacy leaking, they choose to disregard the worries in favour of convenience

- Patching Security Vulnerabilities

  Security experts discover vulnerabilities and exploits, which are then recorded in a database. Then, they are ranked from lowest to highest threat level on a scale of 0 to 10, with 0 being the lowest threat level and 10 representing the highest. When system software on devices is not updated and a vulnerability or exploit is discovered, a problem may occur. An entry point to a whole system could be made via an exploitable device in a network. If the gadget is a component of a smart city, the smart city is exposed. Regular or automatic software updates are the only way to address these kinds of problems. There is one exception to automated patching. Patches should

always be tested in an offline development environment before being applied to a live system. A patch may make modifications that need involvement, or may modify the functionality of a device, for example, a protocol version update may interfere with device compatibility.

4. Recommended Secure Architecture

In smart cities, a large amount of data is being produced every day. The Internet of Things (IoT) architecture, which uses heterogeneous networks (HetNets) [7], serves as the backbone for smart cities. With a robust and secure design, smart cities will be able to flourish more and promote sustainable development practices. Black Networks (BN), Trusted Software-Defined Networking (SDN) Controller, Unified Registry (UR), and Key Management System (KMS) make up the four IoT architectural elements of smart cities. Each of these architectural elements is crucial to the architecture, which generally focuses on HetNets communication and authentication.

3.4.1. 4.1. Black Networks

The meta-data that is associated with the IoT protocol is frequently protected in smart cities via Black Networks. Black Networks essentially give a sense of confidentiality, integrity, and authentication in its networks which cause smart cities to thrive more in terms of network safety. A safe communication can be achieved by encrypting data in the Link and Network Layer. The stream cyphers that can do so include Grain128a or AES in the EAX or OFB modes. Additionally, the meta-data may be individually encrypted in the Network Layer using 6LowPan or ZigBee. The act of encrypting the data in the Link and Network Layer shields smart cities from any network or cyber-attacks.

3.4.2. 4.2. Trusted Software-Defined Networks (SDN) Controllers

SDN creates flexible and effective networking by using software-based controllers that make it simple to distinguish the network layers. Trusted SDN Controller typically secures the communication between networks efficiently through numerous protocols, for example OpenFlow (OF) protocol. OF protocol is a standard inSDN architecture that allows a safe communication between SDN controllers and network devices to take place. The SDN Controller collects data, which is then translated into entries and given to the OF, who then sends the entries to the switch.

3.4.3. 4.3. Unified Registry

Various entities have different functionalities in order to establish an IoT device [36]. A Unified Registry is used to unify the many IoT networks' devices in a Smart City. UR is the key to a successful connection of devices, sensors, and servers. A Visiting Unified Registry can be done as one of the efforts to achieve IoT nodes that are mobile and cross networks [7]. Although the issues involved in implementing UR that include security and legal risks are not to be swept under the rug so easily, establishing a logical entity would be beneficial.

3.4.4. 4.4. Key Management System

In IoT, it is important to establish a reliable Key Management System (KMS) in order to manage the cryptographic keys in a cryptosystem. The system includes replacing keys, creating and transferring data, and crypto shredding which is the ‘deletion’ of data. The concept of data protection is carried out, particularly when dealing with sensitive data. Prior to the IoT lifecycle, KMS is designed where the location and method of key management are specified. Cryptosystems involve two types of keys that includes asymmetric-key and symmetric-key. Asymmetric keys typically offer greater security, albeit having a significant computational burden. However, issues with an IoT environment's key management can be resolved by employing the symmetric key.

5. Conclusion

In conclusion, smart cities are a concept rooted in the implementation of ideas for natural resource management and sustainable and user-friendly architecture. The smart city concept must be practiced with the common consent of the people to ensure that the country can catch up with other countries so as not to continue to fall behind. In the pursuit of a smart city, there are security issues that need to be taken care of so that it does not affect the city's reputation as a smart city. Due to the widespread use of smart devices, security and privacy issues have become more crucial and call for practical solutions. Furthermore, it is essential to consider security and privacy concerns when developing and

implementing new smart systems. In this paper, firstly, we have discussed about architecture of smart cities. Then we go more details about the application of smart cities. There are also some security and privacy issues in smart cities' application that have been discussed. Therefore, there are the solutions for security and privacy solutions in smart cities environment. Then, we discussed about the recommended secure architecture and lastly about the unanswered questions and potential future research areas.

Acknowledgment

The Computer Network and Computational Intelligent Kuliyyah of the Information Communication Technology Department at the International Islamic University Malaysia has provided this article with their full support.

References

[1] C. Grison *et al.*, "Integrated Water Resources Management in Cities in the World: Global Challenges," *Water Resour. Manag.*, vol. 37, no. 6–7, pp. 2787–2803, May 2023, doi: 10.1007/s11269-023-03475-3.

[2] C. Rochet, *Smart Cities*. Wiley, pp. 1-206, 2018, doi: 10.1002/9781119507321.

[3] E. Ahmed *et al.*, "The role of big data analytics in Internet of Things," *Comput. Networks*, vol. 129, pp. 459–471, Dec. 2017, doi: 10.1016/j.comnet.2017.06.013.

[4] R. Bryant, R. Katz, E. Lazowska, Y. Zheng, F. Liu, and H.-P. Hsieh, "Big-Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science and Society," *Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discov. data Min. - KDD '13*, pp. 1–15, 2013, [Online]. Available at: https://cra.org/ccc/wp-content/uploads/sites/2/2015/05/Big_Data.pdf.

[5] J. L. Hernandez-Ramos *et al.*, "Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions," *IEEE Secur. Priv.*, vol. 19, no. 1, pp. 12–23, Jan. 2021, doi: 10.1109/MSEC.2020.3012353.

[6] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1718–1743, 2019, doi: 10.1109/COMST.2018.2867288.

[7] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for Smart Cities," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2016, pp. 812–813, doi: 10.1109/CCNC.2016.7444889.

[8] B. Hamid, N. Jhanjhi, M. Humayun, A. Khan, and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A survey," in *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Dec. 2019, pp. 1–7, doi: 10.1109/MACS48846.2019.9024768.

[9] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and Privacy in Smart Cities: Challenges and Opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, Jul. 2018, doi: 10.1109/ACCESS.2018.2853985.

[10] R. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 32–39, Nov. 2011, doi: 10.1109/MCOM.2011.6069707.

[11] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3677, Mar. 2022, doi: 10.1002/ett.3677.

[12] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A Review of Machine Learning and IoT in Smart Transportation," *Futur. Internet*, vol. 11, no. 4, p. 94, Apr. 2019, doi: 10.3390/fi11040094.

[13] Z. Chen, C. Wang, G. Li, Z. Lou, S. Jiang, and A. Galis, "NEW IP Framework and Protocol for Future Applications," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2020, pp. 1–5, doi: 10.1109/NOMS47738.2020.9110352.

[14] 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.

[15] 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.

[16] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of Privacy in Biometric Data," *IEEE Access*, vol. 4, pp. 880–892, 2016, doi: 10.1109/ACCESS.2016.2535120.

[17] 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.

[18] S. Yu, "Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data," *IEEE Access*, vol. 4, pp. 2751–2763, 2016, doi: 10.1109/ACCESS.2016.2577036.

[19] C. T. Do *et al.*, "Game Theory for Cyber Security and Privacy," *ACM Comput. Surv.*, vol. 50, no. 2, pp. 1–37, Mar. 2018, doi: 10.1145/3057268.

[20] A. A. Alabdel Abass, L. Xiao, N. B. Mandayam, and Z. Gajic, "Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage," *IEEE Access*, vol. 5, pp. 8482–8491, 2017, doi: 10.1109/ACCESS.2017.2691326.

[21] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An Accurate Security Game for Low-Resource IoT Devices," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9381–9393, Oct. 2017, doi: 10.1109/TVT.2017.2701551.

[22] 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.

[23] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017, doi: 10.1109/TSG.2017.2670144.

[24] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-Layer Spoofing Detection With Reinforcement Learning in Wireless Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016, doi: 10.1109/TVT.2016.2524258.

[25] 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.

[26] M. Kearns, M. M. Pai, A. Roth, and J. Ullman, "Mechanism Design in Large Games: Incentives and Privacy," *ITCS 2014 - Proc. 2014 Conf. Innov. Theor. Comput. Sci.*, pp. 403–409, Jul. 2012, doi: 10.1145/2554797.2554834.

[27] 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.

[28] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, Jan. 2018, doi: 10.1016/j.future.2016.11.011.

[29] M. Mohsin, Z. Anwar, F. Zaman, and E. Al-Shaer, "IoTChecker: A data-driven framework for security analytics of Internet of Things configurations," *Comput. Secur.*, vol. 70, pp. 199–223, Sep. 2017, doi: 10.1016/j.cose.2017.05.012.

[30] S.-H. Kim, I.-Y. Ko, and S.-H. Kim, "Quality of Private Information (QoPI) model for effective representation and prediction of privacy controls in mobile computing," *Comput. Secur.*, vol. 66, pp. 1–19, May 2017, doi: 10.1016/j.cose.2017.01.002.

[31] O.-J. Lee, H. L. Nguyen, J. E. Jung, T.-W. Um, and H.-W. Lee, "Towards Ontological Approach on Trust-Aware Ambient Services," *IEEE Access*, vol. 5, pp. 1589–1599, 2017, doi: 10.1109/ACCESS.2017.2663407.

[32] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046–21056, Aug. 2017, doi: 10.1109/ACCESS.2017.2734681.

[33] 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. 121–135, 2012, doi: 10.4067/S0718-18762012000300011.

[34] 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.

[35] 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.

[36] C. Sarkar, S. N. A. U. Nambi, R. V. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying IoT applications," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Mar. 2014, pp. 508–513, doi: 10.1109/WF-IoT.2014.6803220.