Exploring Cyber Security Measures in Smart Cities

Rami Mustafa A. Mohammad
rmmohammad@iau.edu.sa
Department of Computer Information Systems
College of Computer Science and Information Technology
Imam Abdulrahman Bin Faisal University
P.O.Box 1982, Dammam, Saudi Arabia

Mamoun Masoud Abdulqader
mmibrahim@iau.edu.sa
Department of Computer Information Systems
College of Computer Science and Information Technology
Imam Abdulrahman Bin Faisal University
P.O.Box 1982, Dammam, Saudi Arabia

Abstract— **Technologies which enhance the quality of everyday lifestyle are increasing rapidly. During their initial development, Internet and network-based services were not built by taking cyber security measures into consideration. The cost of this is still being paid to this day. Nowadays, there are certainly clear need for cyber security requirements for almost all Internet and network-based systems. Several kinds of such systems are normally connected together in unprecedented ways in smart cities. This in fact will complicate the security requirements that should be considered when building smart cities. Yet, the studies on security requirements in smart cities remain to be one of the fields that needs further exploration. This article explores the essential cyber security requirements in smart cities by considering various previous research studies in the field. On top of that, several other recommended security requirements will be introduced as a response to the gaps that continues to be predominating the field.**

Keywords: *Smart Cities, Cybersecurity, IoT, Security Goals, Cloud Computing*

I. Introduction

The concept of smart city is not by any means a new idea. In fact, it has been around for a long time. Smart cities have been essentially introduced for boosting lifestyle quality of citizens. A smart city is usually described as collection of interconnected network-based systems. smart grid, smart transportation, and Smart healthcare are examples of such systems. Further, smart people are an essential component to any smart city. In the literature, there exists a frequent use of the term “smart” for describing network-based solutions which are proposed to be used in “smart” cities. The use of the term “smart” can indicate that the system is connected to a network and may to some extent communicate with the surrounding environment as well as other systems. “Smart” does not necessarily refers to the intelligence of a system by itself. Consequently, the term "smart people" doesn't necessarily describe the advancement of the intellectual level of individuals living in smart cities. It is simply describing the fact that they are connected to a network or more precisely a collection of networks. The information obtained from “smart” people doesn't have limit. For example, smart healthcare systems can easily monitor person's vital signs twenty-four hours a day. Smart traffic systems, on the other hand, can keep track of someone's movements to facilitate much faster and even more streamlined traveling from one location to another. The connectivity sophistication of such systems is vast because they are interconnected in a manner that can't be avoided as it is often an essential factor towards the success of a smart city. The information that can be acquired about any person in the smart city is not restricted to their immediate connection to a system. For instance, the systems that serve the individual including smart cars and smart girds may generate sensitive information. Actually, both systems offer important functions to people. However, the interaction of smart car system, smart home system, and smart grid system might show if a person is actually in the home or not. Such intense use of private information has escalated a different confidentiality, integrity, and availability concerns. The volume of data that is transferred in a smart city is undoubtedly huge. In the event of information leakage or a compromise in these systems, the damages and costs can be very high. Within the next section, this article is going to explore several cyber security solutions. Such solutions focus on providing security of key components of a smart city. Protecting individual’s personal information, securing the way through which data is obtained and processed, and handling the acquired big data. The ultimate goal of this article is to determine standard cyber security requirements in any smart city.

II. Main Components of Smart Cities

This section starts by discussing main technological aspects employed in smart cities. A statistic of smart cities technologies will be provided. Additionally, solutions for a secure smart city will be briefly discussed. Based on these solutions, general security requirements for smart cities will be suggested and listed in the security requirements section.

1. Internet of Things

Internet of things (IoT) is considered that main component of smart cities. It facilitates the concept of smart cities to a great extent. IoT is a network of interconnected appliances that contain embedded sensors that are able to sense the environment such as heat, temperature etc. IoT devices provide connectivity and data at relatively low cost. IoT devices offer convenient low-cost communication that is interactive with the environment. However, this convenience comes with many vulnerabilities. In an attempt to handle the security issues related to IoT, some researchers proposed an overhaul to IoT while others added improvements to

978-1-7281-8855-3/20/$31.00 ©2020 IEEE

existing protocols. For instance, the proposed system in [1] introduces several components those are Unified Registry, Key Management, Trusted Software-Defined Network (TSDN) controller, and Black Networks. The management of IoT Intrusion Detection Systems (IDS) as well as their mobility and other security requirements such as authorization, authentication, accountability, and availability are achieved via the unified registry. As for key management, they proposed a hierarchal key system that is independent for each protocol to obtain efficient key management and security. Trusted SDN handles secure routing and availability. Black networks ensure confidentiality, integrity, availability, as well as security. As mentioned, perversity, IoT devices have many vulnerabilities. It is logical to assume there are many more that are still unknown. According to [2], there has been extensive research in detecting attacks on IoT devices. However, they use signature-based IDS which can only function in a useful manner if the devices are facing a known attack. To overcome this issue, they suggested a machine learning anomaly-based IDS designed specifically to identify IoT zero-day attacks.

Communication is the backbone of a smart city. Many entities need to communicate in order for a smart city to function properly. Nonetheless, this communication should be regulated. Therefore, Sasaki et al., [3] introduced an access control architecture for IoT. The access control makes sure that just an authorized entity may have access to the data in a specific domain. Moreover, the system they proposed is flexible and allows data access to different yet related domains. At the same time, it ensures privacy. Additionally, it limits the access between domains operating in different fields. For example, the smart traffic control system should get access to data in the smart traffic volume system. However, they should not be able to access information in the smart health care system. Continuing in the area of communication regulation Mick et al., [4], introduced Light weight Authentication and Secured Routing (LASeR). As the name suggests, the protocol provides authentication and routing functionalities while ensuring security in both aspects. The simulation results show that this protocol is light on IoT devices and has minimal overhead.

It is important that the data received from IoT devices is trusted and accurate. Li et al., [5] Proposed a scheme where each node is assigned a trust level. The goal is to mitigate the risk of false information whether it is caused by an attacker that was able to compromise a device, or a malfunctioning unit. As mentioned previously, the paper aims to find security requirements for smart cities. Since IoT is the building block of smart cities, it is essential to set up the security requirements of IoT devices. Several IoT security requirements can be cited here, including:

- Standardization: Having a standard for IoT devices is critical. utilizing the same standard for IoT, will yield improvements in many areas especially security.
- Privacy: The paper discussed privacy concerns regarding IoT. In Both [1, 3] there are solutions to this issue.
- Physical security: A security mechanism must be implemented to prevent physical damage to IoT devices.
- Network Security: To ensure data loss prevention in case of network congestion or interference.
- Tamper Resistance: In case a device was physically compromised by an attacker, the device should maintain security requirements.
- Dynamic Cognitive Spectrum: The big number of IoT equipment in a smart city along with the limitation of the spectrum introduces availability issues. Spectrum limitation is a major challenge. Kusumawati et al., [6] stated that it is expected to have congestion in the 500MGhz frequency range in Jakarta. This issue will eventually become a global one. It can be inferred from the paper that the allocation of a spectrum to be only used for IoT is preferred, and in the future very much needed.

A number of surveys have been performed by researchers in IoT and its relation to smart cities with regards to security. Datta & Sharma [7] investigated 23 papers that show case security solutions. The research analyzed solutions in relation to protocols, architectures, and security of IoT and smart cities. The main take of the research is that, even though there are still some issues, it can be stated that IoT devices have the capacity to be fairly secure if implemented correctly. Latif & Zafar [8] stated that the research in IoT, given the 46 papers in their study, does not provide solutions "in real sense". They mentioned a number of issues that, in their opinion, were not provided with proper solutions. Some of these issues are not security related thus, the focus will be on the security issues listed in the paper. The security concerns as well as research papers that offered a solution are shown in the Table I.

TABLE I: SECURITY ISSUES LISTED IN [11] AND SOLUTIONS IN THE LITERATURE

Security issues	Solutions in The Literature
Availability	[1]
IDS	[2, 9]
Routing Attacks	[1, 4]
Data confidentiality	[3, 4]
Authentication	[1, 9]

Secure and Smarter Cities data management (SMARTIE), is an EC-Funded project. It is an entire secure platform for the protection of sensors or devices. It enables an access control for resources. Additionally, the new design provides secure data storage and processing. The system has many components. Only the ones with direct connection to security will be mentioned. In SMARTIE, the components are divided into groups. Under each group there are several protocols. The groups and protocols that are related to security are as follows:

A. Security Functional Group

- Distributed Capability-Based Access Control (DCapBAC): Authorization strategy which performs access control decision before accessing the service.
- Ciphertext-Policy Attribute-Based Encryption (CP-ABE): Encryption mechanism that does not require data to be encrypted more than once. The mechanism ensures that all the receivers of the data are able to decrypt it.
- XACML with JSON: is used with CP-ABE to provide detailed authorization polices.
- A Lightweight Pseudorandom Number Generator for Wireless Sensor Networks (lmRNG): A lightweight

cryptographic pseudo random number generator for low-powered devices.

- IMASC: An integrity framework which ensures that low-powered devices run in a trusted environment
- Distributed Kerberos: With DCapBAC, it provides light capability token for authentication and authorization. It is designed to prohibit a compromised device from computing a capability token.
- IDS: Scans, finds, and reports undesired behavior to the network administrator.

B. Communication Functional Group

- Lightweight secure CoAP (lwsCoAP): which provides security to data in transmission. lwsCoAP utilizes Elliptic curve. The key size can increase or decrease depending the security requirement as well as the processing power of the device in question.
- IoT Service Functional Group
- PrivLoc: Informs the owner about the location of the assets and whether it entered or exited a pre-defined area.
- TinyDSM: Provides availability in case of a malfunctioning node.
- Privacy-Preserving event detection and correlation: Ensures that the encrypted data remains private by analyzing the data and using limited information to be able to utilize services. This feature can be set by the user depending on their security needs.

The solutions of security issues for smart cities utilize a number of technologies. In the literature, different technologies are implemented together to provide a security solution for a smart city. For example, in some studies, IoT is coupled with machine learning or the cloud to provide a security solution. However, the main focus was on IoT. As a result, it is categorized in the current research under the IoT section.

C. Blockchain

Blockchain is seen as a set of blocks which are connected together by making use of cryptography. Each block contains transaction data, hash value of previous block, and a time stamp. Blockchain is secure by design in terms of integrity. The idea of blockchain is somewhat similar to a linked list. In general, blockchain offers low cost but good security. It is efficient and can be used in many applications with IoT such as authentication. Blockchain can also be used as public key infrastructure (PKI) to achieve authentication. Estonia is one of the countries that offer its citizens a blockchain-based ID. Regardless of some limitations, many tasks can be performed using the digital ID. There are some legal issues with the implementation of blockchain in citizenship authentication. When a citizen utilizes any service that requires them to use their digital ID, the action is recorded. It is difficult to remove the record when it is stored in the blockchain. This goes against General Data Protection Regulation law (GDPR) where an individual has the right to delete his records [10].

In the area of improving security of blockchain, Kotobi & Sartipi [11] noted that the use of blockchain security protocol with a hybrid system, introduced less delay. They defined two main terms in their study. Cloud system which has high processing power, and minor units that is more powerful than IoT devices but offer less power than the cloud. The hybrid system utilizes both cloud and minors to achieve the best performance with minimal delay. Due to the nature of blockchain in the sense that is decentralized, it is not an easy task to set it up for the scale of a smart city. Malik et al., [12] offered a new blockchain platform that addresses security challenges in a smart city. Additionally, they have developed a script that is able to automate the process of creating blockchain for smart cities.

2. The Cloud

The term cloud can be defined as a set of computational and networking recourses that are provided as a service. It is offered on demand and provides the users with scalability to suit their needs. IoT's main job is to generate data. The data generated is useless unless it is collected, processed, and analyzed. Therefore, the cloud is used to perform these actions. The security of the cloud is as important as the security of IoT. There are several risks that are associated with the use of the cloud. The vast number of users in addition to the amount of data being processed are some examples. Due to the large amount of data and users, maintaining availability is a challenge. Moreover, the cloud environment, in case it is shared which is most likely, introduces possible compromises to confidentiality. Traditional risks that already exist in current systems and are going to be ported over to cloud systems in smart cities are also an issue. Information leakage, malicious applications, and unsecure authentication mechanisms, in which an attacker can bypass, are some examples of such problems in relation to the security of the cloud. Therefore Li et al., [13], introduced a security strategy that utilizes encryption, access control that provides secure authentication, and auditing capacities. Based on these risks mentioned above and the security strategy, the study detailed a secure design that deals with the security issues mentioned earlier. In another attempt to mitigate risks of the cloud, Khan et al., [14] proposed a framework that overcomes security issues in relation with the cloud implementation of a smart city. The framework only utilizes open data and data that is offered willingly by citizens. Moreover, the framework ensures privacy, security, and addresses trust issues. In the previous sections, the paper listed IoT, Block chain, and the cloud as the main technologies used in smart cities. The paper summarized the security solutions for their implementation in smart cities. The goal is to describe the solutions in a simplified manner to show case the efforts of researchers in this field as well as the security contributions to smart cities. Table II shows the number of papers investigated for each technology.

TABLE II: STATISTICS OF THE PAPERS INVESTIGATED

Technology	Research papers
IoT Focused	[1] [8] [7] [3] [2] [15] [4] [5] [16] [9]
Block chain Focused	[10] [17] [18] [11] [12]
Cloud Focused	[13] [14]

III. SECURITY AND PRIVACY

This section investigates important aspects of securing a smart city. Also, it will discuss other issues that contributes to the security of smart city including Data Security, Defense and Security Hardening, and Privacy.

A. Data Security

In simple terms, what makes a smart city "smart" is the shear amount of data that is being gathered, transmitted, and analyzed. All the technologies that are used in smart cities, are implemented to achieve such goal. Once the means are secured, the next step is to look into the security of the data itself. Data is at risk in its entire life cycle. From the second it is created and until it reaches the desired destination, in every step of the way, it is still at risk. Even when data is sorted it is still at risk. Smart cities relay on data, and large amounts of it, to function as envisioned. Inherently, smart cities are continuously at risk. Unless important steps are taken to ensure data security. The process starts with carefully planning what to implement and how to implement it. Ensuring the security of the hardware and software is critically important as well. All the stockholders, governments, business and individuals, need to work together to enhance the security of a smart city. An important element of improving security is raising awareness. When the term raising awareness is used, it is assumed that the target is the laymen. This conception is too limited. Everyone needs to be aware about security risks regardless of their level of expertise. When the United States National Security Administration (NSA) found a vulnerability in Windows message block protocol, they reported the issue to Microsoft. Microsoft put out a patch that fixed the vulnerability. Keep in mind, this is the vulnerability that enabled the ransomware "WannaCry" to function. However, the fix provided by Microsoft was released two months before WannaCry started infecting companies. The companies that were struck by WannaCry most likely had security experts. Were they aware of the patch? From this incident the importance of awareness for laymen and experts both alike, should be realized. Raising awareness and improving security in the technical sense goes hand in hand. In the literature, there are solutions that improves the security of data in a smart city. For example, the authors in [19] proposed a technique for analyzing threats and enhance information security. In the study, experiments showed that there is a reduction of risk. The approach starts with a threat modeling process. In this phase information about the environment is gathered. The information ranges from networking topologies to security policies. Based on the data collected, a threat model is produced. Utilizing the threat model, the system is able to identify threats and risks. The study used the approach on a system. As a result, the risk was reduced from the initial risk factor, produced by their approach by 33%. This was obtained after a month of repeating the same process. In three months, the risk factor was further reduced by 20%.

Information leakage is one of the most damaging events that can happen to a company or an individual. In a smart city the damage is amplified due to the large data available to be leaked if not properly secured. The framework that is proposed in [20] can identify the individual that is responsible for the leakage of data. The source of the data is defined in the paper as "Distributor" and the entity that receives the data as "Agent". In case an agent leaked any data, whether it is intentional or not, the system is able to detect the leakage as well as point out the entity responsible for the leakage. The identification of the leaker is achieved using a probability model that is able, through specific calculations, to identify the leaker with relatively high accuracy rate.

B. Defense and Security Hardening

Cybersecurity is a dynamic field. New vulnerabilities are discovered each day. It is important to stay up to date with the latest security issues and how to fix them. In a smart city, it is more important to do so because of the severe consequences of a compromised system. However, it is a tasking process to realize what is the most important element to secure. Arguably, every element in a smart city is equally important, security wise. Since the compromise of any device can lead to the compromise of the entire city, all the systems in a smart city need to be secured. Regardless, categorizing the criticality and the importance of technologies used in a smart city, yields an organized approach to its protection. Security is considered the most challenging issue of smart cities. Results produced by a system that is developed based on related work, and interviews with experts enforces this statement. The system utilizes decision tables, and fuzzy logic to obtain the level of challenge each aspects of a smart city introduces. As mentioned above, the system ranked security as the most challenging part of a smart city [21]. Table III provides a summary of the study findings.

TABLE III: RANKS OF CHALLENGING ELEMENTS IN A SMART CITY

Smart City Element	Ranking
Smart Security	1
Smart Technology	2
Smart Citizen	3
Smart Energy	4
Smart Mobility	5
Smart Governance and Education	6
Smart Healthcare	7
Smart Infrastructure	8
Smart Buildings	9

In [22], a hierarchal defensive system has been developed. The system can deal with advanced attacks as well as low level attacks, whether the attack is known or not, in Wireless Sensor Networks (WSN). Additionally, the system makes use of chance theory and usage control. The goal of chance theory is to find relations, in a given dataset, and provide meaning to rare events which can be used to improve security. Usage control is an access control. It differs from traditional access control by its ability to continuously perform access control before, during, and after the access is granted. The system incorporates low-level detection, performed by the nodes, and high-level detection, performed by the sink and the base station. The risk is mitigated by the use of TSDN, and Network Function Visualization (NFV). Another approach to develop a defensive system was adopted by [23]. The system was not built to secure one aspect of a smart city. As stated in the study the system was designed to be "holistic approach to model the security of a smart city service". The proposed system is a multi-layer defensive system that has three components. The first layer's functionality is to model the security of the services in a system. The model provides many information one of which is calculated risks of system failure due to existing vulnerabilities in the system. The second layer is an independent system that monitors the services offered by the system for any unwanted behavior and take actions if necessary. The second layer could be a firewall, IDS, and so on. In case the second layer failed, the third layer, made of security operation center, which has security analysts will defend the system. Security modeling is an

important process in ensuring the security of a system. It is critical to incorporate security in the early stages of the system development lifecycle. Doing so will ensure better security at a lower cost [24]. The complexity of a smart city due to many factors one of which is the large number of connected devices, introduce a major security challenge. The use of means to model security of a system or provide it, is difficult to perform without knowing what is exactly on the network. Identifying assets in an automated manner makes the process of modeling the system easier and more efficient. Having a clear identification of assets can be misused by attackers to perform a sophisticated attack.

In [25], a security system for smart cities was purposed. The paper stated that a secure system can be achieved using a strong encryption algorithm coupled with an IDS. In [26] a framework has been proposed that improves the security of a smart city. The work utilizes multi cloud approach. Additionally, the framework introduces a new protocol called Zero-Knowledge Proof (ZKP). ZKP incorporate cryptography using the elliptic curve. The goal of the protocol is to overcome privacy and authentication issues.

C. Privacy

Smart cities aim to enhance the quality of lifestyle for the individuals. Smart grid, smart transportation, and smart health care will make life easier for the citizens of a smart city. In order for these smart systems to function, citizens' personal data need to be collected. The collection of the data will ensure that the service is best suited for the citizen. Additionally, the data can be used to optimize the system of the service provided to achieve maximum efficiency. The use of personal data introduces major privacy concerns. Ensuring the privacy of personal data, is one of the challenges in smart cities. Many researchers proposed solutions to deal with privacy concerns [27, 28, 29]. The importance of ensuring privacy is critically high. The reason is, without privacy people will be unwilling to embrace "smartness" which will result in poor adoption, if any, of smart cities [30, 31]. Privacy should not be an afterthought. It should be integrated in the development life cycle of smart cities. To achieve the previously mentioned benefits of collecting data without compromising privacy, data can be aggregated and anonymized. Instead of collecting the data of a specific home, data of ten homes, for example, can be anonymized and aggregated. As a result, the data does not identify an individual home [30, 32, 33]. Still, the aggregated data can be used to optimize the provided service. This way, both service providers and citizens can get what they want.

IV. DISCUSSION

IoT plays a significant role in enabling smart cities. The IoT security solutions range from a new architecture to a new protocol. In general, there are many solutions to improve the security of IoT. However, there is still a lack of security in IoT. Several solutions were proposed as shown in Table I. However, there is a lack of focus on physical security of IoT which is as critical as any of the security concerns. Additionally, there is the general connection of IoT and low power. This paper argues that this is not optimal thinking. IoT can be powerful in terms of computational power according to the definition of IoT stated earlier. Moreover, it is possible that by the time smart cities are widely adopted, IoT power will increase significantly. Therefore, allowing more demanding security solutions to be applied in IoT. It might be less powerful than other devices, but it might be powerful enough to handle more security mechanisms. It is more accurate to state that some IoT devices are powerful and some are not and there are plenty in between. IoTs might provide enough security for a smart city. However, there is a lack of integration. There is also a deficiency in solutions that cover all aspects of a smart city.

Blockchain is a technology that is secure by design. It is logical to desire its implementation in smart cities. However, the research reviewed in this paper is fragmented in a way that makes it impractical to do so. There are some researchers that state, blockchain can be used to improve security, without explaining in technical terms how it should be implemented exactly. Given the sample size of five papers, it can be argued that the judgment of this paper on the state of blockchain in relation to its implementation in smart city is not practical. However, [18] stated "A significant portion of the actual papers only describe the benefits of use Blockchain to authenticate users, and less portions of the research concentrated on security issues." Two solutions have been mentioned which improve the security of the cloud in a smart city. The cloud, similar to IoT, has the benefit of being an existing technology that have been in use for years. It is most likely that security issues in the cloud will be dealt with before the demand for smart cities start. It is widely used by individuals, companies, and governments.

Data security, countermeasures, and privacy are major concerns. The solutions discussed in literature might be adequate on their own but what is going to happen if they were ingrained into one large system of systems is not sufficiently stated. In general, the security solutions are focused on the security of one technology. This approach negates the idea of a smart city where everything is connected.

In general, having clear security requirements for smart cities, can help future designs of smart cities to be more secure. In general, reviewing several research articles, the following security requirements can be concluded:

- Facilitate secure communication.
- Facilitate secure booting.
- Facilitate security monitoring, analysis, and response.
- Facilitate a secure updating and patching management.
- Facilitate secure authentication, identification and access control.
- Facilitate the protection of data and application.
- Facilitate secure lifecycle management.
- Accommodate redundant path(s).
- Apply encrypted link(s).
- The system has to be validated by using no less than 2 parties.
- Provide automated verification for vehicles.
- Ensure privacy in waste management.
- Incorporate components security.
- Facilitate the job of digital investigator(s).
- Apply end-to-end privacy and security.
- Apply crypto and key management policies for systems that has limited computation and memory.
- Apply a transformative trust system for scalable and secure inter-system interactions.
- Adhere to conceptual and comprehensive security policy standards languages.

- Must have a secure key management system that is able to generate, store, revoke, and change keys
- Handle data generated from IoT devices in different domains such as health, traffic, and businesses while maintaining availability.
- Incorporate a methodology for finding zero-day attack to ensure its security
- Use appropriate robust secure lightweight protocols to communicate with low-powered devices securely.
- Ensure that the method by which devices decide which path to take to communicate with another entity as well as how to store a path or lack thereof should be secure.
- Facilitate monitoring capabilities, in addition to automated means, that can be used by a human administrator to determine abnormal behavior.
- Technologies used in the system must be standardized to improve compatibility and security.
- Giving the limited range of frequencies, the system must implement a method to neglect or minimize and possible collision or congestion to maintain availability.
- Ensure the security of data while stored, in transmission, or in processing.
- The subsystems must maintain security when integrated into one whole system
- Security measures in the system should be in compliance with the relative laws, in case that is a challenge, law makers and experts should work together to update the law appropriately.
- Provide mechanisms that facilitate security auditing.
- The system's security measures must be configured properly to gain the highest security possible.
- The system's access control must be dynamic. It should be able to modify rights and permissions to access any resource before, during, and after the access to the resource.
- The system must be tested validated, and verified for confidentiality, integrity, and availability.

V. CONCLUSION

The paper started by giving an introduction about smart cities. Major technologies utilized in smart cities were thoroughly discusses including IoT, Block Chain, and the Cloud. Additionally, security solutions for each technology were discussed. The paper moved into other aspects of securing a smart city which were data security, defensive measures, and privacy. Then, the paper showed of the literature what is similar to its goal which is finding security requirements for smart cities. Lastly the paper listed its findings. The current study may be considered a starting point for further invistigations that would improve the security of smart cities. The paper strongly recommends that the adoption of smart city should not be rushed. Gradually introducing smartness to services is a better approach. It will allow researchers to optimize security as much as possible before the entire integration of a smart city.

REFERENCES

[1] C. D. W. E. Shaibal, "A Secure IoT Architecture for Smart Cities," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2016.

[2] A. Ibrahim, A. Ali and A. Esam, "AD-IoT: Anomaly Detection of IoT Cyberattacks in Samrt City Using Machine Learning," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019.

[3] S. Takayuki, M. Yusuke and J. Astha, "Access Control Architecture for Smart City IoT Platform," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And*, 2019.

[4] M. Travis, T. Reza and M. Satyajayant, "LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities," *IEEE INTERNET OF THINGS JOURNAL,* vol. V, no. 2, pp. 755-764, 2018.

[5] L. Wenjia, S. Houbing and Z. Feng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cites," *IEEE INTERNET OF THINGS JOURNAL,* vol. V, no. 2, pp. 716-723, 2018.

[6] K. Diah, S. Denny and S. Muhammad, "Spectrum Requirement for IoT Services: A case of Jakarta smart city," in *2017 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, 2017.

[7] D. Parul and S. Bhisham, "A Survey on IoT Architectures, Protocols, Security and Smart City based Applications," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2017.

[8] L. Saba and A. Z. Nazir, "A Survey of Security and Privacy Issues in IoT for smart cities," in *2017 Fifth International Conference on Aerospace Science & Engineering (ICASE)*, 2017.

[9] M. B. Jens, S. Antonio, M. M.Victoria, G. Dan and L. Peter, "SMARTIE Project: Secure loT Data Management for Smart Cites," in *2015 International Conference on Recent Advances in Internet of Things (RioT)*, Singapore, 2015.

[10] N. Jongho and y. K. Hun, "A Study on smart city security policy based on block chain in 5G Age," in *2019 International Conference on Platform Technology and Service (PlatCon)*, 2019.

[11] K. Khashayar and S. Mina, "Efficient and Secure Communications in Smart Cities using Edge, Caching, and Blockchain," in *IEEE International Smart Cities Conference (ISC2)*, 2018.

[12] M. Adeel A., T. Deepak K. and G. Uttam, "Non-Intrusive Deployment of Blockchain in Establishing Cyber-Infrastructure for Smart City," in *SECON 2019 workshop on Security Trust and Privacy in Emerging Cyber-Physical Systems*, 2019.

[13] L. Wang, C. Jing and P. Zhou, "Security Structure Study of City Management Platform Based on Cloud Computing under the Conception of Smart City," in *2012 Fourth International Conference on Multimedia Information Networking and Security*, 2012.

[14] K. Zaheer, P. Zeeshan and G. Abdul, "Towards Cloud based Smart Cities Data Security," in *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, 2014.

[15] M. Vishesh, B. Prakhar, M. Kumar and B. Prasenjit, "Empowering the Security for Iot-Based Communications in Smart City," in *2018 International Conference on Automation and Computational Engineering (ICACE - 2018)*, 2018.

[16] S. Deepti and S. G. Nasib, "Security Requirements of IoT Applications in Smart Environment," in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018)*, 2018.

[17] M. Olga B., R. Rogelio, L. Victor M., B. J. Raul, M. Rocio and O. Alberto, "A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures," in *IEEE International Smart Cities Conference (ISC2)*, 2018.

[18] R. Rogelio, R. José G., L. Víctor M. and M. ,. Juan, "How Digital Identity on Blockchain can contribute in a smart city environment," in *2017 International Smart Cities Conference (ISC2)*, 2017.

[19] W. Paul, A. Amjad and K. William, "Data Security and Threat Modeling for Smart City," in *2015 International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC)*, 2015.

[20] D. Vishal, G. Kishu and K. Ashwani, "A Probability based Model for Big Data Security in Smart City," in *2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, 2019.

[21] R. ,. Mohammad, A. Zainab, J. Ruchin and A. Jawdat, "A framework for evaluation of cyber security challenges in smart cities," in *Smart Cities Symposium 2018*, 2018.

[22] W. JUN, O. KAORU, D. MIANXIONG and L. CHUNXIAO, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities," *IEEE Access,* 2015.

[23] M. NAZEERUDDIN, "A Multi-Tiered Defense Model for the Security Analysis of Critical Facilities in Smart," *IEEE Access,* vol. VII, pp. 152585-152598, 2019.

[24] T. Dipty, K. M. Ashish, C. Amrita and K. ,. Anil, "A Study of Security Modeling Techniques for Smart Systems," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con), India, 14th - 16th Feb 2019*, 2019.

[25] S. Nandita, "Designing cyber security system for smart cities," in *Smart Cities Symposium 2018*, 2018.

[26] D. Hamza, J. Feng and L. Jiamin, "Secure Framework for Future Smart City," in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing*, 2017.

[27] A. Modafar and B. Tasnim, "Framework for managing smart cities security and privacy applications," in *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 2018.

[28] K. SHAHEENA, M. M. R. SK, A. MAJED and A. ATIF, "Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment," *IEEE access,* 2019.

[29] C. LEI, X. GANG, Q. YOUYANG, G. LONGXIANG and Y. YUNYUN, "Security and Privacy in Smart Cities:Challenges and Opportunities," *IEEE Access,* vol. VI, pp. 46134-46145, 2018.

[30] S. Mihai, E. Mircea, T. Lucian, A. Lola, P. M. C. Lucas and P. Marco, "Energy ecosystem in smart cities — Privacy and security solutions for citizen's engagement in a multi-stream environment," in *2016 IEEE International Smart Cities Conference (ISC2)*, Trento, Italy, 2016.

[31] S. Ramya, M. Apurva and S. Priyanka, "Privacy Conscious Architecture for improving Emergency Response in Smart cities," in *2016 Smart City Security and Privacy Workshop (SCSP-W)*, 2016.

[32] A. Nasser H., "Impact of Privacy Issues on Smart City Services in a Model Smart City," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. X, no. 2, pp. 177-185, 2019.

[33] E. David and W. Isabel, "Privacy in the Smart City—Applications, Technologie, Challenges, and Solutions," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* vol. XX, no. 1, pp. 489-516, 2018.