International Journal on Advanced Science Engineering Information Technology

Vol.14 (2024) No. 6
ISSN: 2088-5334

Cybersecurity Implementation on Smart Government in Smart City: A Systematic Review

Muhammad Rakha Rafi Baihaqi [a,*], Sutia Handayani [a], Dana Indra Sensuse [a], Sofian Lusa [b], Prasetyo Adi Wibowo Putro [a], Sofiyanti Indriasari [a]

[a] *Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia*
[b] *Master's degree of Tourism Department, Institut Pariwisata Trisakti, Indonesia*
Corresponding author: [*]muhammad.rakha23@ui.ac.id

***Abstract*— Rapid advances in ICT have now developed in various ways. One of the developments is in Smart Government, which has become a Smart City implementation domain. However, the implementation of a smart government must walk from a cybersecurity point of view to ensure its implementation. This study aims to understand how the implementation of cybersecurity in smart government, especially in smart cities, uses the PRISMA protocol and addresses obstacles and related issues. This approach of PRISMA specifies the implementation of cybersecurity in smart government or cybersecurity in government, smart city, governance, and public service and excludes the duplicate papers that are found in databases. Databases used in this study are Scopus, IEEE Xplore, ACM Digital Library, and ScienceDirect. We found 21 publications that met the criteria and classified the implementation based on the technologies obstacles and issues found in the publications. Based on the classification, the most cybersecurity implementation topic in the smart city was the implementation of an Intrusion Detection System (IDS) in every aspect of the smart city, such as the Fog Layer in Smart city, Smart City Hospital, Internet of Things (IoT), etc. with most publication in 2020 and having incremental from 2022 to 2023. The most concerning obstacle and issue was how to make the availability of the smart city service at a tolerable level when the cybersecurity implementation is implemented. The limitation that occurs in this research is how to address the solution to obstacles and issues from the analysis.**

***Keywords*— Cybersecurity; smart government; smart city; systematic review; PRISMA.**

Manuscript received 22 Jan. 2024; revised 7 Aug. 2024; accepted 18 Nov. 2024. Date of publication 31 Dec. 2024.

I. INTRODUCTION

The development of ICT advances rapidly in various ways. One of the advances of ICT was a smart city, which developed an idea about how ICT could play an active role in developing functions in cities [1]The smart city aims to serve its citizens and improve their prosperity. Various motivations exist for developing smart cities, such as increasing demographics, insufficient funding, environmental sustainability, and economic development. [2].

A smart city has six dimensions, one of which is smart government [3]. The smart government itself is a set of business processes with information technology as a main concept for giving information to provide higher quality citizen services and also to solve complex problems in the public sector [4]. It works by utilizing, implementing, and managing policies and data via ICT and stakeholder collaboration by involvement of citizens and development of policy for delivering services and facilitating communication between different entities to optimize the process and increase public trust [5]. It also requires using the smart devices, agents, and sensors embedded in physical space to ensure real-time data can be provided to the city for further analysis and extraction of knowledge [6]. On implementation of Smart Government in smart cities, many public organizations fail in the digital transformation of smart government [4]. The ones who succeed in the implementation face cybersecurity threats, which in every vulnerable in the smart city, putting the entire city in a risk position [7].

A study has identified smart government technology in smart cities needing cybersecurity security [8]. However, there is no explanation of the cybersecurity implementation technologies needed to secure smart government technology. Only a few studies about implementation technologies in smart cities have focused on threats in cybersecurity areas [9]. To get more deeply conscious and comprehend the implementation of cybersecurity and the issues in smart government in smart

cities nowadays, a systematic literature review is needed. A systematic literature review can understand the frontier of knowledge by understanding the breadth and depth of the existing work for later identification of gaps to push the knowledge frontier [10]. Therefore, this study proposes research questions as follows:

- RQ1. What kinds of cybersecurity implementation in smart government?
- RQ2. What obstacles and issues are found related to cybersecurity implementation in smart government in the context of a smart city?

This paper is structured as follows: Section 2 discusses the materials and method used for systematic literature review and the steps used in SLR. Section 3 describes the results and discussion based on materials and method described. Section 4 describes the conclusions from the discussion and future research.

II. Materials and Method

A. Methodological Framework

This study used a systematic literature review approach to examine previous studies to acknowledge the above research question. The SLR method used in this study is the Preferred Reporting Item for Systematic Reviews and Meta-Analyses (PRISMA). The current PRISMA 2020 checklist consists of 27 items that are included in 7 sections [10]. PRISMA consists of three steps: identification, screening, and inclusion. These steps are shown in Fig 1.

Thematic analysis is conducted to construct the cybersecurity topics discussed in the retrieved publications. This analysis consists of three steps: familiarization with the data, generating initial codes, and generating themes [11]. Then, we group the themes to identify the cybersecurity area in smart government and summarize the obstacles and issues found in each cybersecurity area.

B. Planning the SLR

The planning step to conduct the SLR consists of three things: databases, search keywords, and search criteria. The selection of literature is conducted through searching within databases. The databases used in this study are:

- Scopus
- IEEE Xplore
- ACM Digital Library
- ScienceDirect

Search keywords are formulated to find literature that is related to the study. Search keywords that are used in this study are (“CYBERSECURITY” OR (“CYBER” AND “SECURITY”)) AND “SMART CITY.” The query was then applied to do searching on title, abstract, and publication keywords. The search criteria are defined to find the accurate literature to answer the research questions. The list of inclusion and exclusion criteria is shown in Table 1.

TABLE I
Search Criteria

Type	Criteria	Code
Inclusion	Articles published between 2019 - 2023	IN1
	Articles are written in English	IN2
	Article contains an implementation of cybersecurity in smart government or cybersecurity in government, smart city, governance, and public service	IN3
	Articles published in international journals or conferences	IN4
Exclusion	Cannot get access to the full-text	EX1
	Duplicated papers	EX2
	SLR papers	EX3

C. Implementing The SLR

At the identification stage, the query searches related publications from four databases. From this search, 1560 publications were identified. In the screening stage, the search criteria consist of inclusion and exclusion criteria, which are applied to filter the publications. The quality assessment questions are conducted through filtered publications to retrieve related publications that can answer the research question and achieve the study's objective. The quality assessment questions are shown in Table 2.

TABLE II
Quality Assessment Questions

Code	Question
C1	Are the research objectives clearly stated?
C2	Are the results clearly presented?
C3	Does the research describe the proposed architecture or methodology used?
C4	Is the research SCOPUS indexed?

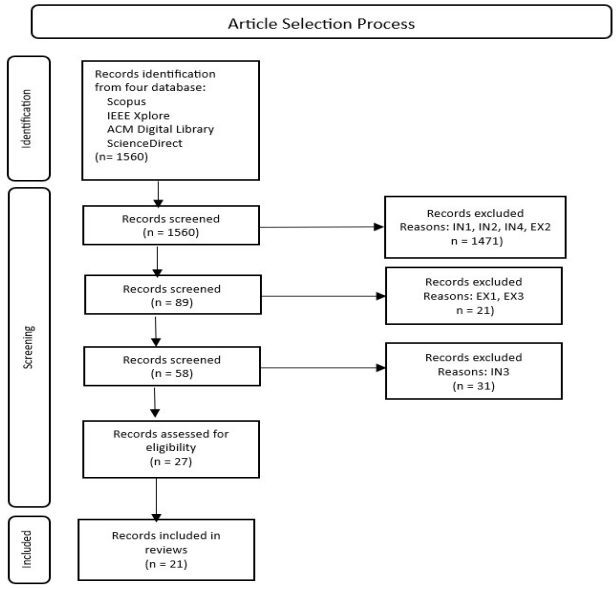

Fig. 1 Research Flow Diagram

III. Results and Discussion

From the SLR process using the PRISMA method that was conducted above by identification, screening, and included phase, we found 21 publications that suit quality assessment questions that have been defined. This final result was filtered by exclusion based on IN1, IN2, IN4, and EX2, screening which excluded EX1 and EX3 and checking the publication which meets IN3. All the phases in the SLR process were conducted collaboratively by authors in an iterative process of

the authors' assessments. Therefore, any difference was discussed until a complete consensus was gained.

We conducted a thematic analysis of these 21 publications to determine what topics were discussed regarding cybersecurity in smart government. Then, we grouped the discussed themes into five cybersecurity topics: Intrusion Detection System (IDS), Cryptography, Security Model, Secure Framework, Law, and Trust Management. Table 3 shows the list of publications discussing cybersecurity and the year they were published.

TABLE III
LIST OF PUBLICATION

Ref	Cybersecurity Topics	Year
[12]	Cryptography	2020
[13]	Intrusion Detection System	2019
[14]	Security Model	2022
[15]	Intrusion Detection System	2023
[16]	Cryptography	2022
[17]	Intrusion Detection System	2023
[18]	Intrusion Detection System	2020
[19]	Security Model	2019
[20]	Intrusion Detection System	2020
[21]	Security Model	2021
[22]	Secure Framework	2020
[23]	Intrusion Detection System	2020
[24]	Cryptography	2021
[25]	Cryptography	2019
[26]	Secure Framework	2020
[27]	Intrusion Detection System	2021
[28]	Intrusion Detection System	2022
[29]	Security Model	2020
[30]	Law	2021
[31]	Trust Management	2022
[32]	Secure Framework	2019

Next, we analyze and discuss each publication above that answers the research question.

A. Analysis of Cybersecurity Implementation

The implementation of cybersecurity in a smart city can be divided into several parts. To answer RQ1, we classified the implementation based on the technology or techniques used. Details of the classification can be shown in Fig 2 and Table IV.

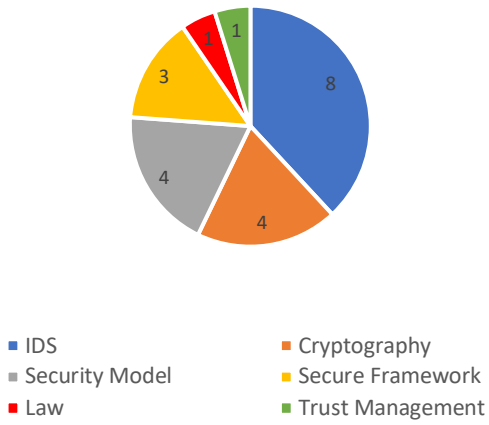

Fig. 2 Cybersecurity Implementation Classification

Based on Fig 2, the implementation of cybersecurity in Smart Cities has the most number of Intrusion Detection System (IDS) topics with eight publications, followed by Cryptography and Security Model with four publications, later in the Secure Framework area with three publications, then Law and Trust Management area with each one publication. The publication shows that cybersecurity implementation in smart cities focuses on detecting attacks that can occur in smart cities. The detection of attacks narrowed into intrusion detection systems, which detect anomalies in smart city systems using different approaches and techniques based on the publication found in the criteria.

From the classification, we analyze the trend of cybersecurity topics based on the year of publication. At least two topics, law and trust management, are excluded because there is only one publication in each area.

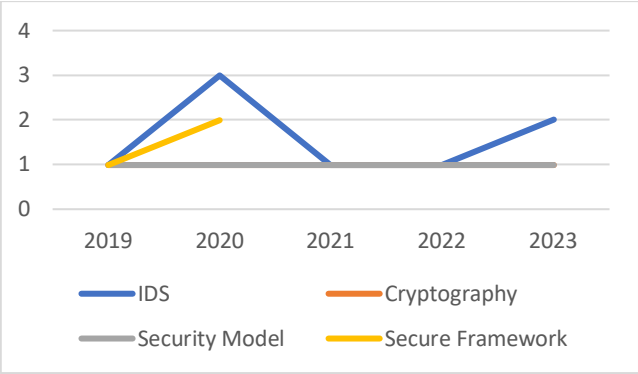

Fig. 3 Year Trend in Cybersecurity Topics

Based on Fig 3, we can show that in 2020, there were the most publications about IDS in smart cities with three publications, followed by 2023 with two publications. This indicates that the publication about IDS was a concern in 2020 and will begin again in 2023. For the Cryptography and Security Model area, the progress of the publication was running constantly, with each year generating one publication. For the Secure Framework area, the publication developed incrementally from 2019 until 2020, with one publication in 2019 and 2 publications in 2020. However, from 2021 until 2023, there was no publication about secure framework topics in smart cities.

TABLE IV
DETAILS CLASSIFICATION OF CYBERSECURITY IMPLEMENTATION

Cybersecurity Area	Implementation	Technology or Techniques
Intrusion Detection System	Fog Layer of Smart City [13]	Machine Learning [13]
	Fog Layer and Edge Layer [15]	Deep Learning CNN [15]
	Bot-IoT Dataset [17]	Some approach of Machine Learning [17]
	Fog Layer of Smart City [18]	ANN Machine Learning [18]
	Dynamic IDS [20]	Data-Driven [20]
	Smart City Hospital [23]	Ensemble Classifier [23]
	SDN DDOS Dataset [28]	Machine Learning and Deep Learning [28]

Cybersecurity Area	Implementation	Technology or Techniques
	IoT [27]	Smart GIS [27]
Cryptography	IoT [12]	Quantum Crypto and Blockchain [12]
	P2P Networks, Smart City Surveillance, Taxi with IoT [16]	Blockhain [16]
	Internet of Vehicle [24]	Elliptic Curve [24]
	Recovering Smart City Critical Data [25]	Blockchain [25]
Security Model	IoT Enabled Smart City [14]	Edge Based [14]
	D2C-ICT Architecture [19]	Anomaly Detection [19]
	IoT in Smart City [21]	Deep Learning and Edge Computing [21]
	Internet of Vehicle (IoV) [29]	Security Threat Model [29]
Secure Framework	Secure Communication [22]	Identity Based [22]
	Software Defined Network [32]	Secure and Agile [32]
	Software Defined Network [26]	Black Networks and Artificial Intelligence [26]
Law	Cybersecurity Law in Smart City [30]	Public Private Partnership [30]
Trust Management	IoT [31]	Fault Tolerant Supervised Routing [31]

The explanation of the cybersecurity implementation described is based on technologies and techniques defined by the implementation.

1) Intrusion Detection System (IDS): Most of the IDS proposed in the studies implement it in the fog layer of smart cities [13], [15], [18] and used machine learning and deep learning technology to detect intrusion by recognizing anomalies. Besides the fog layer, there is also a study that implements intrusion detection on the edge layer [15]. Also, some studies propose the model was built based on already provided datasets such as the Bot-IoT Dataset [17] and DDOS attack SDN and CICDDoS 2019 Dataset [28].

In machine learning and deep learning, preprocessing is one of the essential steps to building a good model. In models where we need to do feature reduction instead of feature selection, Principal component analysis (PCA) can be used. In a study about Smart City Hospital, where the dataset contains symbols that the classifier cannot handle, PCA can be used to do feature reduction that needs to remove the non-numeric or symbol features [23].

Another method to detect cyber security attacks is by using the GeoCluster algorithm with geographic information system (GIS) [27]. The GeoCluster algorithm maps cyber-attacks and intrusion locations. Then, cyber-attack patterns can be explored using advanced spatial statistical analysis and R software. Another study highlights the importance of using data-driven security to protect smart cities [20]. The large amounts of data that smart cities capture, process, and produce can provide a larger data set for better analytics and learning techniques. One application uses it to implement dynamic attack detections.

2) Cryptography: For securing data that flows in a smart city, cryptography can be applied in smart city networks to provide confidentiality, integrity, and data availability. Based on a systematic literature review, this cryptography approach can be applied into the Internet of Things (IoT) [12], Peer-to-Peer Network, Smart City Surveillance, and Smart Taxi with IoT [16], Internet of Vehicles (IoV) [24] , and for recovering critical data in smart city [25]. The implementation of cryptography can be defined again based on techniques such as Quantum Cryptography and Blockchain [12], Elliptical Curve Cryptography [24] and Blockchain [16][25]. The implementation of quantum cryptography and blockchain can be applied in Quantum Key Derivation (QKD), which is enhanced with Discrete Time Quantum Walk-Pseudorandom Number Generator (DTQW-PRNG) where QKD keys become seed for the DTQW-PRNG. With Multiple Attribute Lock Encryption covered by lock chain update protocol, this approach creates multi-level polyvalent data and can be implemented as a polyvalent blockchain. This approach can be applied with traditional blockchain structures such as Merkle Tree to become layered protection of security, which secures the integrity of communication over TCP or personal data and transactions [12].

Implementation of blockchain can be applied by using techniques such as Merkle Hash Tree [25] and can be detailed into Merkle Hash Zero Correlation Distinguisher [16]. However, the purpose of the implementation can be different based on the security needs of the smart city, such as securing data and availability to reduce computational overhead [16] and for recovering critical data from tampering attack [25]. For securing data and availability by using Blockchain Secured Merkle Hash–Zero Correlation Distinguisher (BSMH-ZCD), availability can be fulfilled without decreasing the security strength of the services in Smart city surveillance, Peer-to-Peer Networks, or Smart Taxi with IoT [16]. For recovering critical data using Merkle Hash Tree, the recovery process can be applied when data tampering is detected and can locate the tampered node and data of the blockchain system. This can be done by replicating and storing the critical data from major nodes and then overwriting the data and calculating to validate the recovery node of the smart city [25].

For the Elliptical Curve approach, IoV exchanges messages periodically with their IoV neighbors. The ECC approach helps to secure communication by creating a Certificate Authority (CA) to create Public Key Infrastructure (PKI) for securing communication between IoV. The implementation can be done by linking the vehicle to the owner's private information to make the public and private keys. Later, communication can be done by using the public key of the destination vehicle in the IoV network. ECC can also help IoV by detecting malicious vehicles to prevent blackhole attacks in IoV networks. It can be done using a suspicion level, which continues until the vehicle's trust level is lower than the chosen threshold. For the blackhole attack, it can detect the vehicle that changes behavior over time [24].

3) Security Model: For security model implementation, it develops a cybersecurity standard in smart cities to assure security issues in smart cities. The security model can be implemented in the Internet of Things (IoT) [14], [21], Distribute-to-Centralized ICT (D2C-ICT) [19], and the Internet of Vehicles (IoV) [29]. Techniques that are used for security models are variated, such as Edge Based [14], Anomaly Detection [19], Deep Learning and Edge Computing [21], and Security Threat [29]. For the security model of IoT in a smart city, the edge nodes in a layer in a smart city are used for recommendation-based trust evaluation mechanisms and analysis for isolating the malicious nodes. This model prevents Sybil attacks in which attackers claim different identities to become Sybil nodes to gain access to the smart cities [14]. Another approach, such as Deep Learning and Edge Computing, can be used to prevent unethical activities such as hacked systems, data breaches, and stolen data. Deep learning methods can be developed, such as Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) to model the data and then process it in Edge computing in Edge Layer. The implementation needs security agents to contact IoT devices at the Edge Layer[21].

For D2C-ICT Architecture, the approach used anomaly detection in IoT, Fog, and Cloudlet Layer. The D2C-ICT concept is to make a security layer in the detection process, especially in the cloudlet layer, so attackers have fewer probabilities of entering the cloud layer, which is a central architecture. This approach can detect single node attacks and multi-node attacks by label marking the node into the negative mark and removed from the list of available system resources [19]. For the Internet of Vehicles, the security model can be applied by developing a security threat model to detect cybersecurity threats in Autonomous Vehicle (AV) IoVs. The threat model can be divided based on the security property of information in AV, such as integrity, accessibility, and confidentiality threats. However, this security model implementation of IoV only shows the threat that can occur in the IoV network without the mitigation process [29].

4) Secure Framework: Secure Framework implementation in a smart city can be divided into several aspects in smart city such as Secure Communication [22] and Software-Defined Network[26][32]. For implementation in secure communication, the security framework develops a private key generator (PKG) and pseudonym management authority (PMA) for the safe framework. The PMA is used to generate pseudonyms for identity in the communication party. PKG is used for certificate generation and public and private key generation for secure communication between parties. This approach eliminates the problem of a single point of failure by distributing the task of PGI in multiple levels [22]. For Software Defined Network (SDN), the implementation can use various techniques such as a secure and agile approach [32] and black networks and artificial intelligence [26]. For an agile and secure approach, these techniques are used to prevent DDOS attacks and improve the resiliency of network security in smart cities. The security framework uses a defensive module consisting of D-Defense, C-Defense, and A-Defense. D-Defense is used to detect volume-based attacks on network bandwidth. C-Defense is used to detect the volume-based attack in the control plane. A-Defense is used to detect volume-based attacks on smart city applications. This secure framework approach is practical for smart city applications where the traffic pattern and security requirements are known [32]. These techniques are used for black networks and artificial intelligence to secure the most vulnerable IoT communication. The approach uses the transformation of BLE Data Packet Data Units (PDU) into Black Data PDU by encrypting the data using a stream-based algorithm such as Grain 128-a or AES-EAX mode and then managing using AI engine for management and synchronization of the SDN route lists and patching updates. The secure framework used distributed architectures to lower the risk of single nodes of failures that can occur in centralized architectures [26].

5) Law: The increasing implementation of smart cities that connect more networks provides more digital platforms for digital criminals to conduct crime. Study [30] highlights the importance of the exploration of the alignment of cyber security law with the development of smart cities. This study [30] also proposed a technology-driven law enforcement system that implements a few techniques. This technology-driven response system is enabled automatically based on the crime detection category.

6) Trust Management: Trust management can be implemented to improve trustworthiness and collaborative communication in smart cities. Implementing trust management becomes challenging in smart cities that adopt the Internet of Things (IoT). Lightweight trust management is proposed in [31] that using a supervised IoT-driven system with fault-tolerant secure routing.

7) Obstacles and Challenges: Based on the discussion above, implementing cybersecurity in a smart city will certainly not be without obstacles and challenges. Obstacles and challenges can occur in the implementation processes of cybersecurity in a smart city. We classify the obstacles and challenges based on cybersecurity topics.

Fig 4 shows the obstacles and challenges that occur in implementing cybersecurity in a smart city. Details of the obstacles and challenges are described below.

1) *Intrusion Detection System (IDS):* IDS used a dataset to build the model that can be used to recognize the intrusion. Sometimes, challenges can occur when the dataset is unbalanced [15]Besides that, we must consider that the increase in cyber-attack variations also leads to changes in the features of the dataset. Thus, the change in the dataset might affect the accuracy of the model.

2) *Cryptography:* The Obstacles and Challenges in implementing cybersecurity in cryptography can be defined by how the cryptography approach processes with the environment of the smart city system, such as hardware, computational, etc. This obstacle and challenges can lead to the result of the runtime process and affect the availability of the smart city system [16]. In [25], the approach's limitation is high overhead, which failed when 51% of the significant nodes were compromised and needed hardware for performing computational operations. A similar obstacle can be found in [12] which uses the Quantum approach. The hardware implemented in the smart city system must be confirmed to run Quantum-based in key distribution. For implementation in IoV, it must be confirmed that the availability and delayed information while using secure communication can be

tolerated at the agreed level. This can be a critical challenge and obstacle in IoV because when the availability and delayed information occur at a high level, accidents can happen because when the data is delayed or the availability is low, the IoV is still driving at a constant speed, waiting for the information to be delivered [24].

3) *Security Model:* In the Security Model, obstacles and challenges of the implementation in a smart city can happen when the system's complexity is increased and the data ratio that comes to the security model is increased. In [14] when the complexity of the nodes or load data is increased, the level of the node compromise, data packet drop, misdetection ratio, and average end-to-end delay are increased, too. This causes the packet delivery ratio that comes through the approach security system to decrease. another obstacles and challenges were found in [19] when the system's complexity is increased, more generated prediction models need to be implemented into the system. Also, the implementation of anomaly detection in the cloudlet and fog layers in real cases is not defined. It can cause ineffective hardware to be used for anomaly detection in the security model. When it comes to implementation in IoV, the threat security model in [29] This shows the mapping of the threat and its effect. The obstacle and challenge are how to prevent the threat that has already been mapped in the security threat model. The implementation also faces the challenge of mapping the IoV in a smart city system to show how the nodes of IoV connect to other IoV in the smart city system.

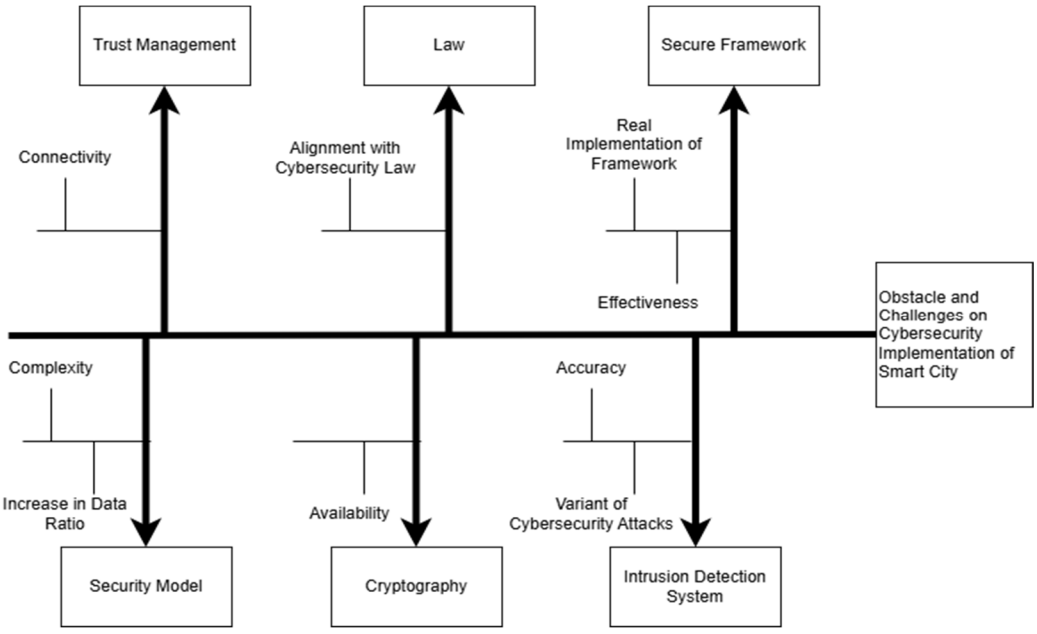

Fig. 4 Obstacles and Challenges in Cybersecurity Implementation of Smart City

4) *Secure Framework:* Implementing a Secure Framework in a smart city faces obstacles and challenges. One of the obstacles and challenges is implementing the security framework in the smart city system. As example in [32]The actual implementation of D-Defense, A-Defense, and A-Defense faces challenges regarding how the framework is implemented and in which layer of the smart city system. The framework's effectiveness is also facing obstacles when implemented in each layer of the smart city system. It can cause a reduction in the availability of smart cities. It also occurred in [32] when AI is used to manage symmetric keys and protect integrity. The availability of the smart city system, especially in critical infrastructure, needs to be maintained to keep the smart city services running well while a secure framework implemented in there still assures the security services provided by the framework [22].

5) *Law:* Only one study explores the enforcement of cyber security law in the implementation of smart cities. Although the study provides that the technology-driven response system can reduce the response system of criminal unit to a very significant degree, the implementation must align with the cyber security law [30].

6) *Trust Management:* Not many studies discussed the implementation of trust management in smart cities. Of all the studies observed, only one study discusses this problem. Trust-FTR model proposed in [31] still has the connectivity problem that occurs when malicious nodes flood many fake packets simultaneously.

IV. Conclusion

This study discusses the cybersecurity implementation of smart government in smart cities and the obstacles and challenges that occur in the implementation. Twenty-one final papers were reviewed using a filtration process using the PRISMA protocol. Based on the review, cybersecurity implementation of smart government in a smart city can be defined and classified into several implementations such as IDS, Cryptography, Security model, Secure Framework, Law, and Trust Management. Most of the implementation of cyber security topics is IDS in smart cities because malicious traffic and attacker approaches need to be detected for further mitigation. The technology or technique that is used in IDS implementation is machine learning for implementing the IDS.

Most smart city implementations for cybersecurity are on IoT in smart cities.

The issue with implementing cybersecurity in smart cities is the implementation of cybersecurity to ensure the availability of services in smart cities while the security aspects are fulfilled. Another issue that occurs in the implementation of cybersecurity in smart cities is how to keep updated on cyber-attack variations and how technology or techniques can be implemented in cybersecurity implementation. This can affect the accuracy of the implementation when dealing with new variations of cyber-attacks and new technology that is implemented in the cybersecurity implementation. The limitation of this research is the lack of information on how to address the solution to the obstacles and issues from the analysis. Therefore, future research that can be conducted from this research will analyze solutions to problems and obstacles that have been defined above.

ACKNOWLEDGMENT

We thank the E-Government and E-Business Laboratory, Faculty of Computer Science, and Universitas Indonesia for supporting our research.

REFERENCES

[1] J. S. Gracias, G. S. Parnell, E. Specking, E. A. Pohl, and R. Buchanan, "Smart Cities—A Structured Literature Review," *Smart Cities*, vol. 6, no. 4, pp. 1719–1743, Jul. 2023, doi: 10.3390/smartcities6040080.

[2] M. Alamer and M. A. Almaiah, "Cybersecurity in Smart City: A Systematic Mapping Study," *2021 International Conference on Information Technology (ICIT)*, pp. 719–724, Jul. 2021, doi:10.1109/icit52682.2021.9491123.

[3] L. Anthopoulos, K. Sirakoulis, and C. G. Reddick, "Conceptualizing Smart Government: Interrelations and Reciprocities with Smart City," *Digital Government: Research and Practice*, vol. 2, no. 4, pp. 1–28, Oct. 2021, doi: 10.1145/3465061.

[4] D. K. Fu'adi, A. Arief, D. I. Sensuse, and A. Syahrizal, "Conceptualizing Smart Government Implementation in Smart City Context: A Systematic Review*," 2020 Fifth International Conference on Informatics and Computing (ICIC)*, pp. 1–7, Nov. 2020, doi:10.1109/icic50835.2020.9288656.

[5] D. Bastos, A. Fernández-Caballero, A. Pereira, and N. P. Rocha, "Smart City Applications to Promote Citizen Participation in City Management and Governance: A Systematic Review," *Informatics*, vol. 9, no. 4, p. 89, Oct. 2022, doi: 10.3390/informatics9040089.

[6] A. I. Niculescu, B. Wadhwa, and E. Quek, "Smart City Technologies: Design and Evaluation of An Intelligent Driving Assistant for Smart Parking," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 6, no. 6, p. 1096, Dec. 2016, doi:10.18517/ijaseit.6.6.1473.

[7] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Reports*, vol. 7, pp. 7999–8012, Nov. 2021, doi: 10.1016/j.egyr.2021.08.124.

[8] M. Y. Habib, H. A. Qureshi, S. A. Khan, Z. Mansoor, and A. R. Chishti, "Cybersecurity and Smart Cities: Current Status and Future," *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T),* pp. 1–7, Jan. 2023, doi: 10.1109/icest56843.2023.10138843.

[9] N. M. Alzahrani and F. A. Alfouzan, "Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review," *Sensors*, vol. 22, no. 7, p. 2792, Apr. 2022, doi: 10.3390/s22072792.

[10] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2021, doi:10.1136/bmj.n71.

[11] D. Byrne, "A worked example of Braun and Clarke's approach to reflexive thematic analysis," *Quality & Quantity*, vol. 56, no. 3, pp. 1391–1412, Jun. 2021, doi: 10.1007/s11135-021-01182-y.

[12] C.-F. Chiang, S. Sengupta, A. Tekeoglu, J. Novillo, and B. Andriamanalimanana, "A Quantum Assisted Secure Client-Centric Polyvalent Blockchain Architecture for Smart Cities," *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, Jan. 2020, doi: 10.1109/ccnc46108.2020.9045188.

[13] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning," *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0305–0310, Jan. 2019, doi: 10.1109/ccwc.2019.8666450.

[14] R. I. Minu, G. Nagarajan, A. Munshi, K. Venkatachalam, W. Almukadi, and M. Abouhawwash, "An Edge Based Attack Detection Model (EBAD) for Increasing the Trustworthiness in IoT Enabled Smart City Environment," *IEEE Access*, vol. 10, pp. 89499–89508, 2022, doi: 10.1109/access.2022.3200703.

[15] M. Hamdan et al., "A Two-Tier Anomaly-based Intrusion Detection Approach for IoT-Enabled Smart Cities," *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),* pp. 1–7, May 2023, doi:10.1109/infocomwkshps57453.2023.10225834.

[16] R. Patan, R. Manikandan, R. Parameshwaran, S. Perumal, M. Daneshmand, and A. H. Gandomi, "Blockchain Security Using Merkle Hash Zero Correlation Distinguisher for the IoT in Smart Cities," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 19296–19306, Oct. 2022, doi: 10.1109/jiot.2022.3171237.

[17] A. Sharma and H. Babbar, "BoT-IoT: Detection of Attacks in IoT-Cybersecurity for Smart Transportation," *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, pp. 522–527, Jun. 2023, doi: 10.1109/icces57224.2023.10192814.

[18] Md. M. Rashid, J. Kamruzzaman, T. Imam, S. Kaisar, and M. J. Alam, "Cyber Attacks Detection from Smart City Applications Using Artificial Neural Network," *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, pp. 1–6, Dec. 2020, doi: 10.1109/csde50874.2020.9411606.

[19] A. Sinaeepourfard, S. Sengupta, J. Krogstie, and R. R. Delgado, "Cybersecurity in Large-Scale Smart Cities: Novel Proposals for Anomaly Detection from Edge to Cloud," *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, pp. 130–135, Dec. 2019, doi:10.1109/iintec48298.2019.9112114.

[20] N. Mohamed, J. Al-Jaroodi, I. Jawhar, and N. Kesserwan, "Data-Driven Security for Smart City Systems: Carving a Trail," *IEEE Access*, vol. 8, pp. 147211–147230, 2020, doi:10.1109/access.2020.3015510.

[21] M. S. Tahsin, Md. Y. Aziz, T. A. Kabbo, T. Tahsin, N. haque Zumme, and M. I. Hossain, "Data Security Model Using Deep Learning and Edge Computing for Internet of Things (IoT) in Smart City," *2021 19th OITS International Conference on Information Technology (OCIT)*, pp. 381–386, Dec. 2021, doi: 10.1109/ocit53463.2021.00081.

[22] N. Gokul and S. Sankaran, "Identity Based Security Framework For Smart Cities," *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1–4, Dec. 2020, doi: 10.1109/ants50601.2020.9342747.

[23] T. Saba, "Intrusion Detection in Smart City Hospitals using Ensemble Classifiers," *2020 13th International Conference on Developments in eSystems Engineering (DeSE)*, pp. 418–422, Dec. 2020, doi:10.1109/dese51703.2020.9450247.

[24] S. Safavat and D. B. Rawat, "On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5050–5059, Aug. 2021, doi:10.1109/tits.2020.3008361.

[25] V. Mishra, S. S. Yau, and C. Yenugunti, "Recovering Decentralized Critical Archival Data From Tampering in Smart City Environment Using Blockchain," *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 1972–1977, Aug. 2019, doi: 10.1109/smartworld-uic-atc-scalcom-iop-sci.2019.00344.

[26] S. Chakrabarty and D. W. Engels, "Secure Smart Cities Framework Using IoT and AI," *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*, pp. 1–6, Dec. 2020, doi:10.1109/gcaiot51063.2020.9345912.

[27] A. M. Aldabbagh and M. Ilyas, "Smart City GIS Mapping and Analysis of Intrusion Detection," *2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1–4, Sep. 2021, doi:10.1109/icecct52121.2021.9616943.

[28] Ms. D. T. Bennet, Ms. P. S. Bennet, and D. Anitha, "Securing Smart City Networks - Intelligent Detection Of DDoS Cyber Attacks," *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 1575–1580, Dec. 2022, doi:10.1109/ic3i56241.2022.10073271.

[29] V. Promyslov and K. Semenkov, "Security Threats for Autonomous and Remotely Controlled Vehicles in Smart City," *2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, pp. 1–5, May 2020, doi:10.1109/icieam48468.2020.9111907.

[30] M. I. Ali and S. Kaur, "The Impact of India's Cyber Security Law and Cyber Forensic On Building Techno-Centric Smartcity IoT Environment," *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, pp. 751–759, Feb. 2021, doi: 10.1109/icccis51004.2021.9397243.

[31] K. Haseeb, T. Saba, A. Rehman, Z. Ahmed, H. H. Song, and H. H. Wang, "Trust Management With Fault-Tolerant Supervised Routing for Smart Cities Using Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22608–22617, Nov. 2022, doi:10.1109/jiot.2022.3184632.

[32] N. Z. Bawany and J. A. Shamsi, "SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks," *Journal of Network and Computer Applications*, vol. 145, p. 102381, Nov. 2019, doi: 10.1016/j.jnca.2019.06.001.