Exploring The Viability And Effectiveness of Lightweight Cryptographic Techniques in Enhancing The IoT Data Security of Smart Cities

Conference Paper · July 2023

DOI: 10.1109/CISES58720.2023.10183537

2 authors, including:

Shraiyash Pandey
Purdue University West Lafayette
11 PUBLICATIONS **58** CITATIONS

SEE PROFILE

Exploring The Viability And Effectiveness of Lightweight Cryptographic Techniques in Enhancing The Iot Data Security of Smart Cities

Shraiyash Pandey
School of Engineering and Technology Sharda University,
Greater Noida, India
shraiyash.pandey@gmail.com

Bharat Bhushan
School of Engineering and Technology Sharda University,
Greater Noida, India
bharat_bhushan1989@yahoo.com

2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) | 979-8-3503-2391-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/CISES58720.2023.10183537

***Abstract*—Smart cities have evolved into a new model that provides a better quality of life, and efficiently optimizes the resources in the city to provide improved facilities. However, despite the evolution of smart cities, privacy and security challenges are a concern that needs to be addressed. Therefore, in this paper, we thoroughly explore the complications that arise in the protection of data in smart cities, and the various lightweight cryptographic algorithms available that can be implemented as a viable and feasible solution. Smart cities are immensely equipped with IoT devices, therefore we present various accessible methods to protect the data of IoT devices, which indirectly results in the protection of data in smart cities. The paper aims to provide various lightweight cryptographic algorithms and methods available that are suitable for the security of smart cities. Moreover, explain the challenges towards the implementation of each algorithm to exploit all challenges of smart city security. Each algorithm provides a certain level of security in its own manner, however, no algorithm can be defined as ideal and perfect for all types of cyberattacks, so we present a comparison among various algorithms that can be implemented. Further, we present a list of recent advancements in the security of smart cities to provide extensive information on recent innovations, new security models, new communication protocols, new authentication schemes, etc. which are all under the same domain of security of smart cities.**

Keywords*—*Smart City, Security, Lightweight Cryptography, Internet of Things

I. INTRODUCTION

"Smart city" is the implementation of different technologies and services in a smart and structured way with the initiative of creating interconnected, functional, and efficient major cities [1]. More importantly, smart cities offer an experience of an enhanced standard of public services and improved operational effectiveness to all citizens. Smart cities consist of different layers and pillars that form the overall architecture and structure. Smart cities offer a great set of applications in modern society. For instance, smart sources of energy for the consumption, generation, and monitoring of information with the help of IoT devices in smart cities. Smart cities offer smart healthcare, smart education, and smart security to all citizens. Smart cities are highly dependent on Blockchain, Artificial Intelligence (AI), Internet of Things (IoT), etc., which are some available technologiesin the market [2,3].

The security of data in smart cities is crucially important and required especially when data is stored in mostly IoT devices. The current IoT devices, which are held accountable for the collection of data from various sources and sending it to storage facilities via the currently existing systems, increase the system vulnerabilities and provide a possible entryway for malicious intruders to infiltrate the system. The standard of intelligent systems in smart cities can be diminished by malicious nodes and devices launching various types of attacks. Such attacks aim to gain access, eavesdrop on two different parties, and block authorized parties from services and systems. Many existing security protocols may be applied to smart cities, however, due to the storage of data and real-time analysis of data in high volume, they are unable to effectively safeguard the information. Additionally, it is crucial to develop the proper security techniques for smart cities due to the rise of some clever attacks, such as cold boot attacks, and Man-In-The-Middle, which can highly disrupt the confidentiality of citizens [4, 5]. Therefore, smart cities can receive many intruders which raises concerns for the security of smart cities. Therefore, smart cities that offer so much to modern society need to be protected with the uttermost security protocols. Such protocols can be developed with the help of cryptography.

Cryptography, developed using various mathematical principles and sets of computations known as algorithms, is a well-known communication method to secure data from intruders. Cryptography converts plain texts, or messages, in various ways, therefore it becomes difficult to decipher [6]. Cryptography algorithms are used for safe and secure communication that's highly confidential such as transactions from credit cards, cryptographic key generation, safe web browsing online, digital signing, email, etc. On the other hand, Advanced Encryption Standard (AES), Data Encryption Standard (DES) [7], and Rivest Shamir Adleman (RSA) are algorithms in cryptographic applications which are advancing in terms of improved performance [8]. Smartwatches, smartphone applications, radio frequency identification (RFID) tags, etc., are IoT devices that typically focus on basic information processing. As a result, both the physical size and computational capacity of devices are typically small, e.g., low random-access memory (RAM), slow data transmission, limited storage, operating on battery, etc. Therefore, IoT devices cannot dedicate a significant amount of memory and computing power solely to security protocols, unlike tablets, desktop computers, and other similar devices. At that point, the need for lightweight cryptography (LWC), a less-complex variant of traditional cryptography, emerged [9]. This variant anticipates using a limited number of computational cycles to perform encryption methods while maintaining high resilience against cyber threats. Overall, LWC is an emerging varaint of the traditional cryptography implemented in smart cities which is best suited for resource constrained devices. Maimut et al. [10] presented various solutions based on lightweight cryptography for the privacy and security of Radio-

Frequency Identification (RFID) tags, which are used in IoT. RFID tags are used for the primary purpose of communicating, seraching, tracking and identifiying people and items with the help of radio frequency. Lightweight cryptography solutions are advicsed due to the constraints in power consumptin, bandwidth, and memory in RFID tags. Dar et al. [11] proposed the use of blockchain to protect the data being exchanged from Smart Hand-held devices to Cloud networks and vice versa in smart cities. To allow data communication, the data is encrypted digitally with a system generated public-priave key pair. Therefore, it encourages communication devices to use the blockchain stored keys to encipher data. Gunathilake et al. [12] highlights different issues and applications that arise in lightweight cryptographic techniques for IoT devices in smart cities. Zhang et al. [13] presented a tag verfication and tag embedding PH-Y layer authentication which is lightweight in nature for IoT devices in smart cities. The major contributions of this work can be enumerated below.

- This paper presents the different layers present in the architecture of smart cities and the four pillars or infrastructures that make up a smart city.
- This paper highlights the complications that arise in the protection of data in smart cities and various cyber attacks that appear in smart cities.
- This paper presents a comparison among various lightweight cryptographic algorithms available that can be implemented as a viable and feasible solution.

II. SMART CITIES

Technologies such as Artificial Intelligence (AI), Geographic Information System (GIS) Technology, Internet of Things (IoT), and Blockchain are implemented in smart cities to enhance operational efficiency, provide fast and easy dispersion of information to the residents, and overall better standard of living. That's how a smart city differentiates from an average city. By adopting such technologies and data analysis, a smart city seeks to improve residents' quality of life, optimize municipal operations, and foster economic development.

A. Architecture of Smart City

The Architecture of Smart Cities consists of four different layers with specific duties and elements. Each layer of the architecture is discussed below:

- Sensing layer: The firstmost layer, consisting of different objects and elements to obtain information through the surrounding environment such as resources of traffic, homes, and smart cities.
- Data Collection layer: The data gathered from the previous layer is transmitted via either wireless or wired communication to specific databases. Such databases are responsible for the storage of data received.
- Data processing layer: The data stored in databases then needs to be processed, which happens in the data processing layer. Batch processing and real-time processing are two essential duties of this layer. However, it's difficult to process such large-size data with the traditional algorithms since traditional algorithms are better suited for average and normal-size data that is within limited defined data sets. Therefore, complex algorithms are required to process such a high volume of data efficiently.
- Smart Processing layer: This layer is one of the most crucial layers in the architecture of smart cities since it must exchange data from smart applications and operators. On the other hand, the smart processing layer also performs accurate data analysis to make important decisions.

B. Pillars of Smart City

The four essential elements or also known as infrastructures that make up the Pillars of Smart City [14, 15], as shown in Fig. 1, are discussed below:

- Institutional Infrastructure: Planning, management, and governance within a city with the focus of involving residents in making decisions have pertained to basic activities in the institutional infrastructure. It is crucial to analyze data on a real-time basis to ensure such decisions don't include any prejudice and arbitrary behavior.
- Physical Infrastructure: Indicates using Technology to combine efficient and cost-effective physical infrastructure, for example, efficient energy consumption, and very fast internet.
- Social Infrastructure: Consists of a variety of mechanisms for supporting the development of social and human capital as well as the provision of a smart, user-friendly, and connected infrastructure.
- Economic Infrastructure: It includes the basic amenities and services that facilitate the creation and delivery of commercial activities and help create the required infrastructure for higher job employment rates and gather investments.

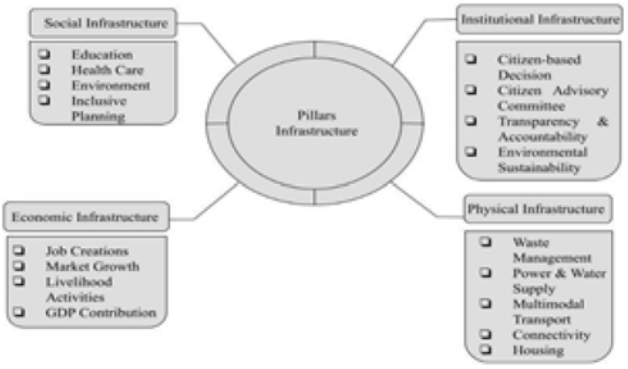

Fig. 1. Pillars of Smart City

C. Smart City Security Issues

IoT devices are in command of information storage and infromation communication because there are hundreds and thousands of interlinked IoT devices within every smart city. Therefore, malicious attackers can take advantage of the framework of smart cities to develop and spread software that can spread across numerous interconnected networks. As a result, intruders can quite easily get access to private data, including users' bank and healthcare details. In addition, intruders can launch various cyberattacks with various objectives in mind, as shown in Table 1. Firstly, to alter the system settings and data, for example, a SQL injection attack where the intruder acquires unlawful access to confidential

data and modifies the data. Secondly, to shut down or restrict access to the system for permitted parties, for example, Denial-of-Service (DoS) is a type of attack that denies service to authorized parties. Lastly, to extract the information, track system activities, and eavesdrop on two communication parties, for example, Man-In-The-Middle attack where an intruder may be able to eavesdrop on the communication between a client and host [16].

TABLE I. VARIOUS CYBER ATTACKS

Type of Attack	Objective of Attack
SQL Injection	To alter the system settings and data
Denial of Service	To block entry of the system or shut it down for authorized parties
Password Attack	To gain unauthorized access of a system
Man-in-the-Middle Attack	To read or steal data as it travels between two devices
Phishing Attack	To gain access of confidential data
Code Injection Attack	To manipulate stored data in the database
Zero-Day Exploit	To perform malicious and unauthorized behaviour in the software or application

III. LIGHTWEIGHT CRYPTOGRAPHY IN SMART CITY SECURITY

A communication and secure information technique developed using mathematical principles and a group of computations, referred to as algorithms, is known as Cryptography. The technique modifies communications (cipher) in various ways, making it extremely difficult to crack down or decipher. The goal of cryptography is to create algorithms or methods that continue to carry out specific duties even in the existence of an attacker. Giving users the ability to speak privately and authentically over a secure route is one of the fundamental tasks of encryption. Cryptography's main function is the protection of data. Usually, that data lies within IoT devices. IoT devices can range in various sizes, externally and internally, therefore, it's difficult to develop a security protocol that is ideal and suitable for all IoT devices. To address the security issues and expand several applications of cryptography for resource-constrained systems, lightweight cryptography is introduced. It is a form of encryption method that consists of low computational complexity is introduced [17].

Systems such as Mobile applications, Radio Frequency Identification (RFID) tags, and IoT gadgets are resource-constrained systems since such systems acquire low RAM, limited internal memory, are battery-operated, have slow data rates, etc. Thus, resource-constrained systems cannot afford to dedicate a significant amount of memory and computing power solely to security protocols. Therefore, a less-complex variant of traditional cryptography, lightweight cryptography, was a perfect fit for such systems' security functions. This version of cryptography anticipates using a small number of computational cycles to perform cryptographic algorithms, offering high resilience against security threats. Internet of Things network data is secured with the implementation of lightweight cryptography methods in smart cities. The IoT network data is secured using lightweight cryptographic algorithms, where such algorithms can either be symmetric or asymmetric. Lightweight Block Cipher (LWBC) is a widely known lightweight cryptographic algorithm derived from the symmetric lightweight algorithm. And, Lightweight Stream Cipher (LWSC) is also another symmetric lightweight algorithm. However, both symmetric algorithms have their own technique to process data. And, on the other hand, an example of asymmetric cryptography is Elliptic Curve Cryptography (ECC). The number of cycles, key size, structures, and block size is used to assess the lightweight cryptographic primitives' contributing factors. Three distinct cipher technologies are used to protect data in smart cities: stream cipher, block cipher, and elliptic curve cipher.

A. Lightweight Block Cipher (LWBC)

One type of symmetric lightweight cryptographic encryption is the block cipher, which processes an entire block of data simultaneously. Two different types of networks, Feistel network (FN) and Substitution Permutation Network (SPN), implement lightweight block ciphers in their network. Feistel structure employs the same course and same program code for both encrypting and decrypting information. However, when it uses the same course, it has less difference in the length of plain text and encrypted text. And, when it uses the same computer code, it guarantees low memory consumption [18]. However, there's also a Generalized Feistel Network (GFN), which consists of different variants that can be implemented for various symmetric lightweight ciphers. SPN structures are better suited because they require fewer processing rounds and use less electricity [19]. Without a key schedule, the SPN network is quicker, leaving the system open to assaults.

B. Lightweight Stream Cipher (LWSC)

A different type of symmetric lightweight cryptographic method that follows the concept of encrypting and decrypting data bit for bit is the stream cipher. Stream ciphers are easier to implement and faster in terms of computational time than block ciphers. It is widely used in Wireless Sensor Network (WSN), and smartphones [20]. Due to the fast processing time and less computation time, the use of stream ciphers is common for the security of IoT data. The stream ciphers, Salsa20, Chacha, RC4, and Trivium are a few popular options amongst the other symmetric lightweight cryptographic algorithms to choose from.

C. Lightweight Elliptic Curve Cipher (ECC)

ECC guarantees both confidentiality and verification [21]. Since asymmetric ciphers require a bigger size of the key and higher memory, they are less common in IoT security but still implemented. IoT network security implements asymmetric cryptography algorithms such as ECC and RSA. ECC offers more cryptographic strength with the use of smaller key size to demonstrate comparable security to RSA. IoT systems can be secured using the Diffe-Hellman and El-Gamal key scheme. According to the processing time on microcontrollers that are of 8-bit, AES is approximately 100–1000 times faster compared to ECC [22]. The most widely used lightweight cipher for offering security in an IoT device is ECC.

D. Symmetric and Asymmetric Lightweight Algorithms

Several different algorithms exist for both symmetric and asymmetric lightweight algorithms. The comparison amongst various symmetric algorithms is structured on the

block size, key size, and the structural network used to implement the algorithm. The asymmetric algorithms are not widely used in IoT security due to the specifications of the key size, thus more time and memory consumption. However, different asymmetric algorithms compare with one another based on encryption and decryption attributes. A Comparison of a few symmetric lightweight algorithms is shown in Table 2. Following, many symmetric and asymmetric lightweight algorithms are discussed below.

Advanced encryption standard (AES), TWINE, CLEFIA, and HIGHT are all different symmetric lightweight algorithms [23]. AES's encryption process works on a 4X4 matrix that consists of blocks sized 128-bits and implements the SPN. The organization of the internal state for AES is done by addroundkey, subbyte, mixcolumn, and shiftrows. TWINE makes use of the Feistel structure that is invoked eight times every cycle and the XOR operation is performed on the 4X4 S-Box and the sub key. TWINE is a more complex iteration to speed up dispersion as compared to High Security and lightweight (HIGHT) Height [24]. HIGHT uses a very straightforward and fundamental operation to function for the Generalized Feistel structural network. That is, during encryption and decryption, a key is generated. Similarly, CLEFIA also functions for the GFN, however, the block size of CLEFIA is 128-bits as compared to 64-bits of the HIGHT.

RSA and Elliptic curve cryptography (ECC) are two asymmetric lightweight algorithms that are similar in terms of key size but differ in cryptographic strength. RSA is not entirely considered a lightweight cryptography algorithm due to its large key size, and provides less cryptographic strength with the same key size in comparison to ECC. ECC is the other asymmetric lightweight algorithm that implements the algorithm with a smaller key size, therefore, it needs less memory space and offers improved processing speed [25]. As a result, it is used in a limited region of a hardware application, which speeds up real-time processing. Overall, ECC offers a much greater level of cryptographic strength compared to RSA for the same key size.

TABLE II. COMPARISON OF VARIOUS SYMMETRIC LIGHTWEIGHT CRYPTOGRAPHIC METHODS

Methods	Classification	Block Size (Bits)	Key Size (Bits)	Network
AES	Symmetric	128	128,192,256	SPN
TWINE	Symmetric	64	80	FN
CLEFIA	Symmetric	128	128,192,256	GFN
HIGHT	Symmetric	64	128	GFN

IV. NEED OF LIGHTWEIGHT CRYPTOGRAPHY IN SMART CITY

LWC is still in the development stage. However, to move towards the fulfillment of data processing requirements for 5GN smart cities, there is an urgent requirement for effective LWC techniques. Networking with minimal energy consumption, high-speed transmission, affordability, and minimal latency are all the features that lightweight cryptography offers to meet the needs of 5GN smart cities to prevent threats and attacks. A requirement for LWC that relies on very few computing resources, less memory space, and longer battery life all with minimal power consumption is best suited for smart city and IoT devices used in smart cities. Data protection and insurance of privacy are also important domains to be protected with more efficient and effective lightweight cryptographic algorithms in smart cities. Data protection involves encryption and decryption of data that leads to the access of the data stored.

A. Challenges in the Implementation of Appropriate LWC Algorithms

As easy as it sounds, implementing and developing such lightweight cryptographic algorithms that meet all the requirements to protect data and offer optimized results is very challenging. Several reasons explain that explain the critical challenges faced to ensure privacy in smart cities. Firstly, IoT devices are not able to compute more complex algorithms since the CPU is minimal. Secondly, since most IoT devices operate on limited battery power, the power usage of security protocols should be minimal. Thirdly, to cover a massive physical network, the simple sensors are interconnected to each other. Finally, to implement the security protocol algorithm in most devices, the cost should at minimal. However, lightweight cryptography algorithms such as AES [26, 27], RSA, and DES do not apply applicable to such smart fields due to the dynamic features of smart cities and scalability. These algorithms operate on high energy consumption, therefore, would not work with most IoT devices. Therefore, to handle such challenges, there is a requirement for more appropriate cryptographic algorithms that are compatible and feasible for smart devices that are constrained to resources, computational power, size, power supply, memory, etc. Traditional cryptographic primitives are not suited best for such cases and therefore lightweight cryptographic algorithms perform high-security methods of encryption and decryption with low-power applications and preservation of computational power.

V. RECENT ADVANCEMENTS

Mohamed et al. [28] proposed the implementation of data-driven security to provide security for smart city systems. Alotaibi et al. [29] proposed the use of an authentication scheme in smart cities for E-governance systems. Butt et al. [30] presented an approach to guarantee safety and security in the setting of smart cities by introducing a new method that relies on determining and predicting hotspots for crime in smart cities. Karie et al. [31] presented a review of current security protocols and assessment frameworks to discover potential resolutions of the security demands in smart sectors of IoT. Lu et al. [32] proposed a communication protocol to protect data transmissions with strong and extremely lightweight encryptions that involve symmetric cryptography-based key scheme. Suresh et al. [33] presented an authentication security protocol that fights against various popular cyber attacks. Sanjuan et al. [34] proposed a security protocol with the implementation of Cryptographic Smart Cards to resolve the authentication, data privacy and integrity problems in smart cards. The major advancements in the Security of Smart City Applications are abridged in Table 3.

TABLE III. MAJOR ADVANCEMENTS IN THE SECURITY OF SMART CITY APPLICATIONS

Reference	Year	Major Contribution

Reference	Year	Major Contribution
Mohamed et al. [28]	2020	Proposed to improve the security of smart city systems with the help of data-driven security
Alotaibi et al. [29]	2022	Proposed the implementation of an authentication scheme in smart cities for E-governance systems.
Butt et al. [30]	2021	Proposed a new method based on determining hotspots of crime to predict the place of cyber-attacks and their prevention
Karie et al. [31]	2021	Presented a review of current security protocols to discover resolutions to security demands
Luo et al. [32]	2020	Proposed a communication protocol to protect data transmissions with strong encryptions
Suresh et al. [33]	2022	Presented an authentication that fights against various popular cyber attacks
Sanjuan et al. [34]	2020	Highlighted the need for a security schema in the MQTT protocol

VI. Conclusion and Future research Directions

In conclusion, after describing and classifying smart city research areas, we identified the need for strict and efficient security protocols to improve security from different perspectives. Moreover, we presented the architecture and pillars of a smart city followed by its security issues and challenges. Depending on various IoT devices in smart cities, we critically reviewed potential security protocols for previously identified issues and challenges that would fit appropriately and ideally for the security of IoT data. The solutions are based on lightweight cryptography; therefore, we presented the difference between traditional cryptography and lightweight cryptography, and the reason to implement LWC rather than its traditional approach. LWC is a perfect approach towards the security of smart city devices with constrained resources of power, size, and battery. The requirement of LWC, its present situation and difficulties in that current situation, suitable technologies such as -AES, TWINE, CLEFIA, and HIGHT, and the three methods of LWC have all been addressed in this paper by assessing the scientific and practical studies that have already been done in academia.

Future research can be done towards analyzing more recently developed block and stream ciphers in terms of efficiency and feasability for resource constrained devices in smart cities. For instance, Ascon and Elephant are two lightweight block ciphers recently developed, and Spirtz along with NORX are two popular stream ciphers stream ciphers which have also been recently introduced to provide security for resource constrained devices and are lightweight in nature. Analyzing such ciphers for particularly the security of smart city devices can be an initiative for future reserach directions.

References

[1] J. M. Barrionuevo, P. Berrone, and J. E. Ricart, “Smart cities, sustainable progress,” IESE Insight, vol. 14, pp. 50–57, 2012

[2] A. Zanella, ‘‘Internet of Things for smart cities,’’ IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, Feb. 2014.

[3] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, “Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges,” J. Netw. Comput. Appl., vol. 181, May 2021, Art. no. 103007, doi: 10.1016/j.jnca.2021.103007.

[4] J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and S. A. Shah, ‘‘A timeefficient approach towards DDoS attack detection in IoT network using SDN,’’ IEEE Internet Things J., early access, Jul. 19, 2021, doi: 10.1109/JIOT.2021.3098029

[5] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, “Security and privacy in smart city applications: Challenges and solutions,” IEEE Comm. Magazine, vol. 55, no. 1, pp. 122–129, 2017.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, pp. 145–195, March 2002.

[7] H. P. Alahari and S. B. Yelavarthi, "Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT," Third International Conference on Inventive Systems and Control (ICISC), 2019, doi: 10.1109/ICISC44355.2019.9036403. IEEE.

[8] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, doi: 10.1109/WF-IoT.2019.8767250. IEEE.

[9] B. J. Mohd and T. Hayajneh, “Lightweight block ciphers for IoT: Energy optimization and survivability techniques,” IEEE Access, vol. 6, pp. 35966–35978, 2018.

[10] D. Maimut and K. Ouafi, "Lightweight Cryptography for RFID Tags," in IEEE Security & Privacy, vol. 10, no. 2, pp. 76-79, March-April 2012, doi: 10.1109/MSP.2012.43.

[11] M. A. Dar, A. Askar and S. A. Bhat, "Blockchain based Secure Data Exchange between Cloud Networks and Smart Hand-held Devices for use in Smart Cities," 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Jeju Island, Korea, Republic of, 2022, pp. 457-460, doi: 10.1109/ICAIIC54071.2022.9722646.

[12] N. A. Gunathilake, W. J. Buchanan and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: : Implementation, Challenges and Applications," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 707-710, doi: 10.1109/WF-IoT.2019.8767250.

[13] P. Zhang, J. Liu, Y. Shen, H. Li and X. Jiang, "Lightweight Tag-Based PHY-Layer Authentication for IoT Devices in Smart Cities," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3977-3990, May 2020, doi: 10.1109/JIOT.2019.2958079.

[14] UNCTAD, “Smart cities and infrastructure,” Tech. Rep., 2016. [Online].Available:http://unctad.org/meetings/en/SessionalDocuments/ecn162016d2 en.pdf

[15] B. Cooper and D. Rawat, “Cyber security—A necessary pillar of smart cities,” Ernst & Young, London, U.K., Rep., 2016. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cybersecurity-a-necessary-pillar-of-smart-cities.pdf

[16] D. E. Levy-Bencheton, C ´ edric, “Cyber security for smart cities- ´ an architecture model for public transport,” European Union Agency For Network And Information Security, Tech. Rep., 2016. [Online] Available: https://www.enisa.europa.eu/publications/smartcities-architecture-model/at download/fullReport

[17] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[18] R. Kousalya and G. A. S. Kumar, "A Survey of Light-Weight Cryptographic Algorithm for Information Security and Hardware Efficiency in Resource Constrained Devices," International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019, doi: 10.1109/ViTECoN.2019.8899376. IEEE

[19] B. S. Sumit Singh Dhanda, Poonam Jindal, "Lightweight Cryptography: A Solution to Secure IoT," Wireless Personal Communications, 2020, doi: 10.1007/s11277-020-07134-3. Springer.

[20] M. J. R. Shantha and L. Arockiam, "SAT_Jo: An enhanced Lightweight Block Cipher for the Internet of Things.," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), 2019, doi: 10.1109/ICCONS.2018.8663068. IEEE

[21] W. Stallings. Cryptography and network security: principles and practice. Pearson Education India, 2003.

[22] F. Shaikh, E. Bou-Harb, N. Neshenko, A. P. Wright, and N. Ghani, "Internet of Malicious Things: Correlating Active and Passive Measurements for Inferring and Characterizing Internet-Scale

Unsolicited IoT Devices," IEEE Communications Magazine, vol. 56, no. 9, pp. 170-177, 2018, doi: 10.1109/MCOM.2018.1700685. IEEE.

[23] E. R. Naru, H. Saini, and M. Sharma, "A recent review on lightweight cryptography in iot," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Feb 2017, pp. 887–890.

[24] Lee JH, Lim DG (2014) Parallel architecture for high-speed block cipher, HIGHT. Int J Sec Appl 8(2):59–66

[25] Eisenbarth T, Kumar S (2007) A survey of lightweight-cryptography implementations. IEEE Desi Test Comput 24(6):1–12

[26] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight cryptography for embedded systems – a comparative analysis," in Data Privacy Management and Autonomous Spontaneous Security, J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Foley, and W. M. Fitzgerald, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 333–349.

[27] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen, "Design and implementation of low-area and low-power aes encryption hardware core," in 9th EUROMICRO Conference on Digital System Design (DSD'06), Aug 2006, pp. 577–583

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

[29] S. S. Alotaibi, "Registration Center Based User Authentication Scheme for Smart E-Governance Applications in Smart Cities," in IEEE Access, vol. 7, pp. 5819-5833, 2019, doi: 10.1109/ACCESS.2018.2884541.

[30] U. M. Butt et al., "Spatio-Temporal Crime Predictions by Leveraging Artificial Intelligence for Citizens Security in Smart Cities," in IEEE Access, vol. 9, pp. 47516-47529, 2021, doi: 10.1109/ACCESS.2021.3068306.

[31] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.

[32] X. Luo et al., "A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment," in IEEE Access, vol. 8, pp. 67192-67204, 2020, doi: 10.1109/ACCESS.2020.2978525.

[33] D. Suresh, V. Odelu, A. G. Reddy, K. Phaneendra and H. S. Kim, "Provably Secure Pseudo-Identity Three-Factor Authentication Protocol Based on Extended Chaotic-Maps for Lightweight Mobile Devices," in IEEE Access, vol. 10, pp. 109526-109536, 2022, doi: 10.1109/ACCESS.2022.3205290.

[34] E. B. Sanjuan, I. A. Cardiel, J. A. Cerrada and C. Cerrada, "Message Queuing Telemetry Transport (MQTT) Security: A Cryptographic Smart Card Approach," in IEEE Access, vol. 8, pp. 115051-115062, 2020, doi: 10.1109/ACCESS.2020.3003998.