International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Lightweight Cryptography based Communication Model for Device Identification, Mutual Authentication, and Encryption in a Smart City Environment

Md Shamsul Haque Ansari[1], Monica Mehrotra[2]
[1]Jamia Millia Islamia University: Department of Computer Science
New Delhi, India
shamsshamsul@gmail.com
[2]Jamia Millia Islamia University: Department of Computer Science
New Delhi, India
drmehrotra2000@gmail.com

Abstract— Providing security to smart city networks is one of the challenging and demanding tasks in the present days, due to its increased utilization in smart intelligent transportation systems. For this purpose, there are various security protocols and mechanisms that have been developed in the existing works, which targets to establish the reliable and secured communication in smart city networks. However, it limits the major issues of increased computational cost, communication cost, storage overhead, and reduced efficiency. In order to solve these problems, the proposed work intends to design an intelligent security framework by using the Light-weight Cryptography based Communication Model (LCCM). Proposed framework includes the modules of setup initialization, vehicle registration, authentication, key generation, encryption, and decryption. Here, the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are performed with reduced cost complexity. For guaranteeing the security of networks, the random value-based key generation, data encryption, and decryption processes are performed. During the performance analysis, various evaluation measures have been used to assess the results of both convention and proposed security protocols. This paper presented a new methodology named as, LCCM for enhancing the security of smart city transportation networks.

Keywords-Smart City Systems, Security, Lightweight Cryptography Model, Random Value Generation, Key Generation, Authentication, Vehicle-to-Vehicle (V2V) Communication, and Vehicle-to-Infrastructure (V2I) Communications.

I. INTRODUCTION

Smart Cities [1, 2] are becoming more popular and extensively used in many application systems such as smart citizens, transportation, smart water, energy, building, urban services, home, and waste collection. Among other applications, smart intelligent transportations [3] have gained a significant attention in the present days, due to its increased energy efficiency, reduced time consumption, and autonomous communication strategy. Typically, the smart cities [3, 4] are originated from the source of Information and Communication Technology (ICT), which supports the sustainable development processes. According to recent reports, it is studied that the Internet-of-Vehicles (IoV) [5] is an advanced technology developed based on the combination of inter, intra, and vehicular intelligence systems. This infrastructure allows an efficient communication between the vehicles, sensors, road side unit, etc. as shown in Fig. 1. However, providing security [6-8] to these systems is more essential for protecting the network against unauthorized access. For this purpose, various security mechanisms are developed in the work, which are related to the trust-based model, authentication-based model, and cryptographic model.

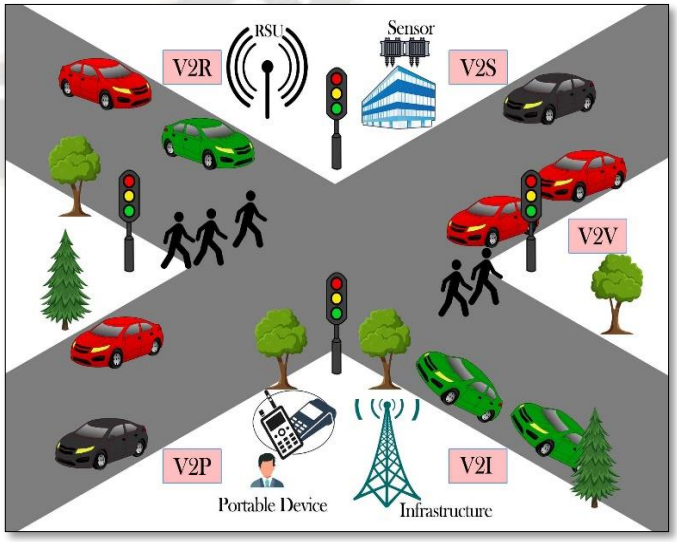

Figure 1. Architecture of smart city systems

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

For ensuring the security of smart city networks, the following requirements need to be satisfied: data anonymity, freshness, confidentiality, authentication, resistance to attacks, and reliable. Yet, it facing the problems [9, 10] of high complexity in operations, requiring more time consumption, increased storage cost and communication cost. Hence, the proposed work intends to develop a new security framework for enabling reliable and secured data communication in smart city networks.

The main contributions of this research work are as follows:

- To establish the secured communication in smart city networks by developing a Lightweight Cryptography based Communication Model (LCCM).
- To assure the reliable and valid data transmission between the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications with reduced communication cost, computational cost, and storage overhead.
- To increase the level of security, the random value-based key generation and encryption processes are performed with the corresponding security parameters.
- To validate the performance of this scheme, different performance evaluation measures are computed and compared with other recent state-of-the-art models.

The remaining portions of this paper are split into the following sections: Section II reviews the existing security mechanisms used in the smart city scenario with its advantages and disadvantages. Moreover, the detailed description about the proposed methodology is presented with its working operations and flow illustration in Section III. The performance results of the proposed security model are validated and compared by using various evaluation metrics in Section IV. Finally, the overall paper is summarized with its future scope in Section V.

II. RELATED WORKS

This section discusses about some of the existing mechanisms related to the machine learning approaches, authentication, and trust models used for ensuring the increased security of smart city networks. Moreover, it discusses about the advantages and disadvantages of each model based on its operating features and characteristics.

Xie, et al [11] presented a comprehensive survey on analyzing various issues and challenges in providing security to a smart city environment. This work analyzed the major impacts of using blockchain methodology for satisfying the security measures of pseudonymity, automation, democracy, and decentralization. Typically, the blockchain is considered as one of the suitable technologies for increasing smart systems like smart healthcare, grid, transportation, and supply chain management. Yao, et al [12] implemented an end-to-end traffic classification model for ensuring QoS of smart city applications. Here, the data flow was constructed based on the matrix model, which helps to optimally minimize the time consumption and increase the generalization ability of smart city networks. The stages involved in this work were as follows: traffic dataset obtainment, preprocessing, matrix construction, feature extraction, and classification. The key benefits of this methodology were increased detection accuracy, optimal time consumption for training, and high efficiency. Still, it is facing the problems of high complexity in computations, and misclassification results due to the redundant features. Li, et al [13] developed a policy-based security scheme for increasing the security of smart city networks. The main purpose of this work was to accurately detect the malicious nodes by generating policies based on the trust value. Moreover, the data fusion was also performed in this work for improving the accuracy of detection by fusing multiple data. Moreover, the level of trust has been estimated for all nodes involved in the network for generating alerts at the time of adversary detection.

The major advantages of this work were increased detection efficiency, precision, and reduced false alarms. Yet, it follows some complicated steps for network operations, and the lack of reliability, which affects the QoS of smart city systems. Dua, et al [14] developed a new message communication protocol for satisfying the security parameters of forward secrecy, privacy, message authentication, and integrity. Here, the BAN logic was also utilized for validating the mutual authentication between the cluster head and vehicles. In addition to that, the real or random model was utilized to assess the semantic security of this framework. The advantages of this work were increased accuracy, reduced delay consumption, and reliable communication. However, it is facing the issues of increased computational and communication overhead.

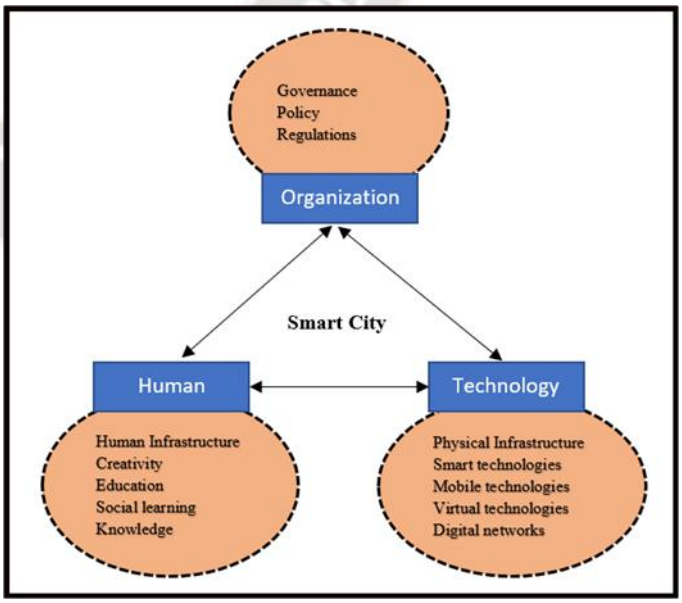

Figure 2. Framework of smart cities

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Moreover, a conceptual framework of smart city networks is shown in Fig 2. Shafiq, et al [15] developed an effective machine learning algorithm for spotting the BoT-IoT attacks in IoT-smart city systems. The key factor of this work was to utilize the machine learning algorithm for accurately detecting the BoT-IoT attacks by using the hybrid machine learning classification technique. Additionally, it validated the performance of various classification techniques such as Bayes Net, C4.5, Naïve Bayes (NB), Random Forest (RF), and Random Tree (RT). Kisseleff, et al [16] presented a comprehensive review on different types of challenges and opportunities for smart city security. Here, the services, platforms, sensors, and communications required for developing smart city systems were investigated. Elsaeidy, et al [17] utilized the deep learning model for accurately detecting the replay attacks in the smart city systems. The contribution of this work was to increase the accuracy of attack detection by using deep learning model.

Jan, et al [18] developed an end-to-end encryption framework for increasing the security of smart city systems with reduced computational complexity. Here, the lightweight symmetric key encryption model, named as AES 128 bit was utilized for ensuring the secured data transmission. This framework comprises the working modules of connection request establishment, cluster head selection, and establishment of secured data transmission. Zhang, et al [19] suggested some security solutions for ensuring the privacy and data security of smart city systems. Sharma, et al [20] employed a blockchain methodology for constructing the hybrid security framework to ensure the reliable data communication and transmission in smart city networks. Saracevic, et al [21] suggested a cryptographic key exchange model for establishing the secured communication between the sender and receiver communicating parties. In this model, the Lattice Path combinatorial approach was utilized to perform the key agreement process, which ensures the security against unauthorized users. Mishra, et al [22] introduced a GraphCrypto model for guaranteeing the data integrity and confidentiality of smart city systems. This framework includes the processes of group formation, secret key generation, encryption, and decryption, where the correctness of the security model has been assessed based on the parameters of complexity and time. However, this model requires increased time consumption for key generation and encryption processes, which degrades the performance of the entire security systems. Rana, et al [23] conducted a detailed review on various lightweight cryptography models used for ensuring secured data transmission in smart city networks. Here, both the symmetric and asymmetric cryptography models have been discussed, which includes the types of block cipher, stream cipher, and elliptic curve cipher. To assess the performance of these mechanisms, various evaluation parameters such as key size, latency, and throughput have been computed.

Based on this review, it is studied that the security models are highly focusing on establishing the reliable and secured data transmission/communication in smart city systems. However, it is facing the problems related to the factors of computational complexity in designing the algorithms, requires more time consumption and lack of flexibility. Hence, the proposed work objects to develop a new security model for ensuring the valid data communication in smart city systems.

III. MATERIALS AND METHODS

This sector presents the clear description of the working methodology with its appropriate block representation and algorithmic illustrations. The key contribution of the proposed work is to perform cryptographic operations with reduced computational time for enabling secured communication in smart city networks. For this purpose, a Lightweight Cryptography based Communication Model (LCCM) has been developed in this work, where the improvement of different factors such as time of execution, storage overhead, and communication cost are highly concentrated. As shown in Fig 3, the proposed security framework comprises the following modules:

- Network construction
- Initialization setup
- Vehicle registration
- Authentication
- Secured communication

A. Network Information

Initially, the network is constructed with the elements of Internet-of-Vehicles (IoVs) components, and server, in which the IoVs are existing in the lower layer and the vehicle server present in the upper layer.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

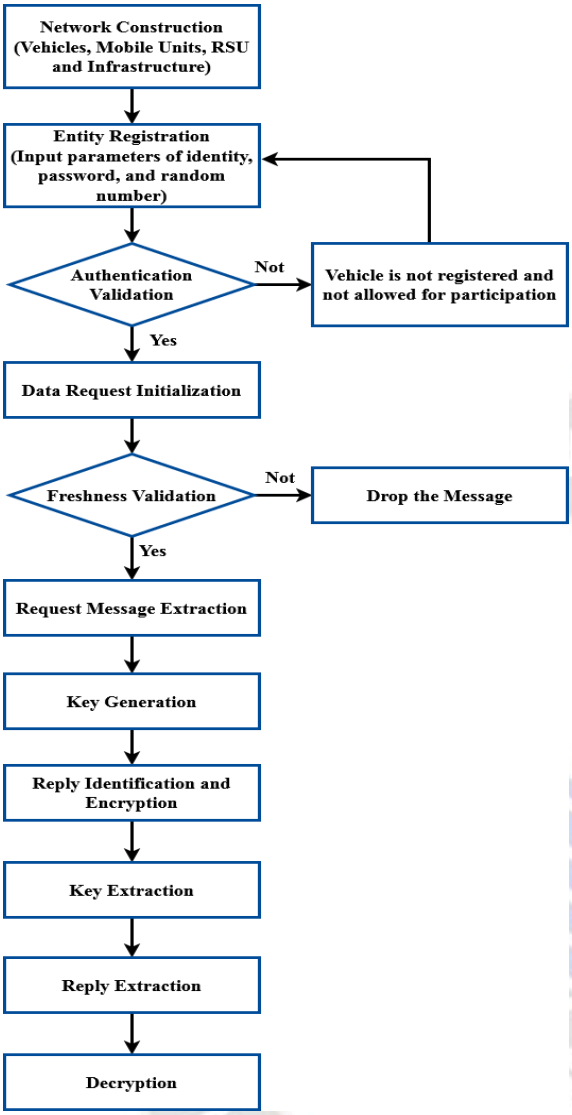

Figure 3. Flow of the proposed LCCM security system

After construction, all communicating participants are got registered through the Transport Layer (TL) protocol. Here, the following assumptions have been taken:

1. In this communication system, the registered vehicles are only allowed for data transmission and communication.
2. Then, the vehicle server VX is considered as the most trustful and authenticated participant, which has increased data storage capability. Hence, it cannot be compromised by other entities or unauthorized users.
3. Moreover, the Road Side Unit (RSU) and other communicating participants are having the storage space for processing.
4. Specifically, registered vehicles or users are not allowed to share their credentials with other participants or unauthorized persons.

Based on these factors, the network is constructed and communication has been established between the communicating elements.

B. Initialization Setup and Vehicle Registration

After constructing the network, all participants are got registered with the server, which generates the precomputed key as shown in below:

$$PK_{VX} = h(R_x||Id_{VX}) \quad (1)$$

Where, PK_{VX} indicates the pre-computed key generated by vehicle server, R_x is the random value generated by vehicle server, and Id_{VX} indicates the identity of the vehicle server. After initialization, all communicating participants such as vehicles, RSU, mobile devices, sensor devices, and infrastructure are registered as follows:

In which, each vehicle in the network is registered with the parameters of vehicle Ve_s, identity of vehicle Id_{Ve_s}, generated password of vehicle PS_{Ve_s} and random value f_s, which is represented in the following format:

$$K_s = h(Id_{Ve_s}||f_s) \text{ and } L_s = h(PS_{Ve_s}||f_s) \quad (2)$$

Then, the generated values of K_s and L_s of vehicle Ve_s is transmitted to the VX via secured medium of channel. In the server side, it estimates the values in the following form:

$$F_s = h(K_s||L_s) \oplus PK_{VX} \quad (3)$$

Consequently, the generated value of F_s is transmitted to requested vehicle through the secured wireless medium. Based on this value, the requested vehicle Ve_s can its smart card as shown in the following form:

$$\{SmC_{Ve_s} = F_s, K_s, L_s\} \quad (4)$$

Similar to this, the RSU can get registered by sending its identity Id_{RT_t} to the VX, which generates the random value r_t for estimating the registration card of RSU as shown in below:

$$B_t = h(Id_{RT_t}||r_t) \oplus PK_{VX} \quad (5)$$

Then, the generated random value r_t and registered card value B_t are transmitted to the appropriate RT_t, which stores the received value for further communication. The mobile devices are registered by sending its identity Id_{MD} to the server VX. To guarantee the security, the server can generate the random value p_u for estimating the registered card value as shown in below:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

$$C_u = h(Id_{MD}||p_u) \oplus PK_{VX} \quad (6)$$

Simultaneously, the generated values of p_u and C_u are send to the requested mobile device MD_u. The sensor device shares its identity Id_{Se} to the server VX that estimates the random value q_v for generating the registered card as shown in below:

$$D_v = h(Id_v||q_v) \oplus PK_{VX} \quad (7)$$

Then, the server sends the values of D_v and q_v to the registered sensor device, which stores the received values for further communication. Finally, the infrastructure shares the identity Id_{IF_k} to the server that computes the random value g_d for generating the registered card as represented in below:

$$W_d = h(Id_{IF_k}||g_d) \oplus PK_{VX} \quad (8)$$

Then, the server shares these values with the registered infrastructure, which stores the received values for further communication.

C. Authentication Based Communication

After registration of all entities participated in the work, the authentication has been done before establishing the communication between these entities. Hence, each vehicle is required to prove its identity and authenticity before sending the request to other participants. In this framework, the reliable communication is established between the entities with ensured data freshness and integrity. When the entity receives the request from each other, it identifies the reply message for the subsequent request and sends the encrypted response message along with the key. In the receiver side, the receiving vehicle can extract the corresponding key for obtaining the decrypted data. During vehicle-to-vehicle communication, if the vehicle S (Ve_s) wants to communicate with vehicle R (Ve_r), it generates the message with the following:

- Input - $Id_{Ve_s}, PS_{Ve_s}, f_s$;
- Generated values - K_s and L_s;
- Select the request - Req_{SR};
- Transmission time - Ti_1;
- Generated random value - a_s;

After that, it transmits in the following format:

$$PK_{VX} = F_s \oplus h(K_s||L_s) \quad (9)$$

$$X_s = h(PK_{VX}||Ti_1) \oplus a_s \quad (10)$$

$$Y_s = Req_{SR} \oplus a_s \oplus PK_{VX} \quad (11)$$

Then, the message X_s, Y_s, Ti_1 is send to the receiver vehicle, which receives the message once that validates the following parameters:

- Receiving time - Ti_2;
- Input - $Id_{Ve_R}, PS_{Ve_R}, f_R$;
- Estimate the values - K_R, L_R;
- Compare the time delay as

$$\triangle Ti_1 \leq Ti_2 - Ti_1$$
$$PK_{VX} = F_R \oplus h(K_R||L_R)$$
$$a'_s = X_s \oplus h(PK_{VX}||Ti_1)$$
$$Req_{SR} = Y_s \oplus a'_s \oplus PK_{VX}$$
$$E_R = h(a'_s||\Delta Ti_1||PK_{VX})$$
$$F_R = E_R \oplus PK_{VX} \oplus a'_s$$
$$EncN_{rly} = Enc_{E_R}(N_{rly})$$

The receiver vehicle sends the encrypted form of reply $\{EncN_{rly}, E_R, Ti_2\}$ to the sender. Consequently, the receiving time Ti_3 between the sender and receiver vehicles are estimated as shown in below:

$$\Delta Ti_2 \leq Ti_3 - Ti_2 \quad (12)$$

$$\Delta Ti'_1 = Ti_2 - Ti_1 \quad (13)$$

$$E'_R = h(a_s||\Delta Ti'_1||PK_{VX}) \quad (14)$$

$$E_R = F_R \oplus PK_{VX}||a_s \quad (15)$$

$$E_R = E'_R \quad (16)$$

$$N_{rly} = Dec_{E_R}(EncN_{rly}) \quad (17)$$

Based on this way, the secured communication is performed between the vehicle-to-vehicle in smart city network. Similar to that, the communication between the vehicle with mobile, RSU and infrastructure are performed in the phases of initialization of data request, ensuring the data freshness, key generation, encryption, and decryption. This type of communication strategy can efficiently improve the performance of entire smart city networks with increased reliability and security measures.

IV. Result And Discussion

This section discusses the performance analysis of the proposed LCCM security protocol by using various evaluation indicators such as communication cost, storage overhead, processing time, response delay, and response loss. Moreover, the obtained results are compared with the recent state-of-the-art models for proving the effectiveness of the proposed model. Table I and Fig 4 compares the communication cost of conventional and proposed security protocols used in the smart

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

city systems with respect to the type of communication. Typically, the communication cost is assessed based on the total number of transferred bytes and stored bytes.

TABLE I. COST ANALYSIS

Security system	Communication Type	Cost
Li, et al [24]	V2R	74.515
Li, et al [24]	V2V	24.835
Li, et al [24]	RSU-V2V	74.505
Wang, et al [25]	V2V	0.021
Jiang, et al [26]	IoT	0.048
Mohit, et al [27]	SVS	0.042
Lee, et al [28]	IoT	0.043
Proposed LCCM	V2V	0.032
Proposed LCCM	V2I	0.032

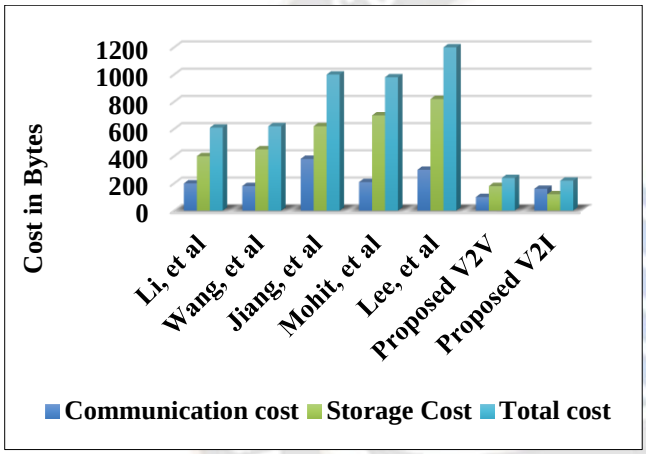

Figure 4. Cost analysis of existing and proposed security models

Based on this evaluation, it is observed that the proposed security protocol requires the reduced cost consumption for both V2V and V2I communications, when compared to the other models. Table II and Table III compares the communication cost and storage overhead of conventional and proposed security protocols during the time of authentication. These parameters are evaluated based on the type of communications V2V and V2I. Typically, the communication cost of smart city networks is estimated according to the number of operations involved in the system that includes the processes of key generation, setup initialization, encryption, and decryption.

TABLE II. COMMUNICATION COST ANALYSIS

Security models	Type of communication	Communication cost
Li, et al [29]	V2V	24.835ms
Wang [30]	V2V	0.020ms
Vasudev [31]	V2V, V2I	7.774ms
IoV-SMAP [32]	V2V	0.034ms
IoV-SMAP [32]	V2I	0.026ms
Proposed LCCM	V2V	0.032ms
Proposed LCCM	V2I	0.024ms

TABLE III. STORAGE OVERHEAD ANALYSIS

Security models	Type of communication	Storage overhead
Li, et al	V2V	450 bytes
Wang	V2V	488 bytes
Vasudev	V2V	192 bytes
Vasudev	V2I	138 bytes
IoV-SMAP	V2V	192 bytes
IoV-SMAP	V2I	138 bytes
Proposed LCCM	V2V	190 bytes
Proposed LCMM	V2I	136 bytes

Similar to that, the storage cost is also computed with respect to the number of computational steps involved in the operations. From these evaluations, it is analyzed that the proposed LCCM technique requires reduced communication cost as well as storage overhead, when compared to the other schemes. Fig 5 and Table IV presents the average processing time of existing [33] and proposed models with respect to varying number of users/vehicles participating in the network.

TABLE IV. AVERAGE PROCESSING TIME OF EXISTING AND PROPOSED SCHEMES

Number of users	BDCA-SDN	IoT-HiTrust	CEF	OSS	Proposed LCCM
20	120	100	90	80	70
40	124	105	95	100	90
60	130	118	100	90	85
80	130	120	110	80	80
100	140	130	130	102	90
120	178	138	138	100	95
140	180	140	170	98	90
160	190	150	140	98	90
180	220	188	158	120	100
200	260	230	160	100	90

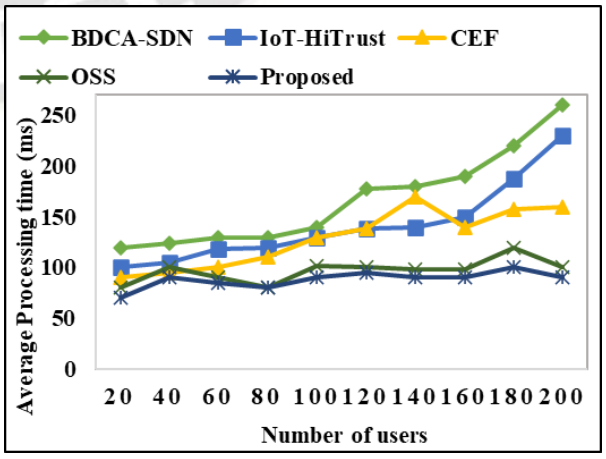

Figure 5. Average processing time

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

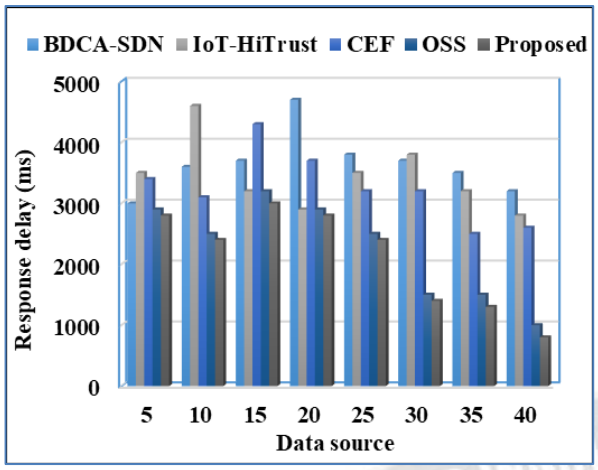

Figure 6. Response delay

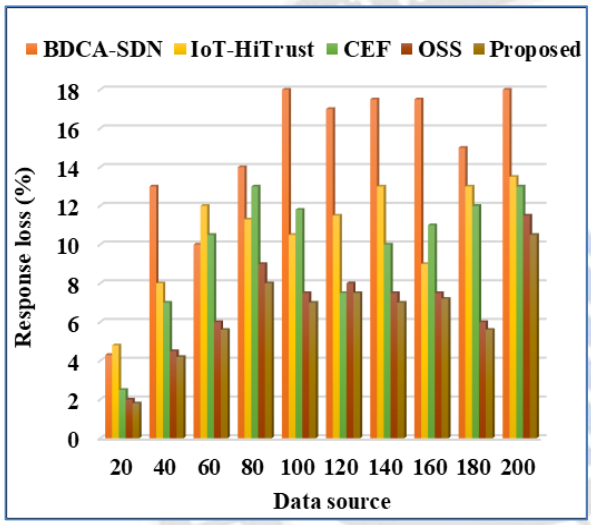

Figure 7. Response loss

Normally, processing time is defined as the amount of time required for sending and receiving messages with a proper response. During communication, the authentication, request selection, encryption/decryption, and transmission operations have been computed, and the total amount of time required for accomplishing these operations at both the sender and receiver side separately is defined by the average processing time. Based on this comparative analysis, it is evident that the proposed security model requires reduced average time consumption over the other state-of-the-art models. Moreover, the response delays of the existing and proposed schemes are validated with respect to varying data sources as shown in Fig 6, and its response loss is analyzed in Fig 7. Then, the values of both response delay and loss are shown in Tables V and VI, respectively. In which, the response delay is determined by how much time the receiver takes for sending response to the requested source with proper authentication.

TABLE V. RESPONSE DELAY OF EXISTING AND PROPOSED SCHEMES

Data Source	BDCA-SDN	IoT-HiTrust	CEF	OSS	Proposed LCCM
5	3000	3500	3400	2900	2800
10	3600	4600	3100	2500	2400
15	3700	3200	4300	3200	3000
20	4700	2900	3700	2900	2800
25	3800	3500	3200	2500	2400
30	3700	3800	3200	1500	1400
35	3500	3200	2500	1500	1300
40	3200	2800	2600	1000	800

Then, the response loss is defined as the loss of message at the time of communication. According to these results, it is observed that the proposed LCCM security protocol provides minimized response time and loss, when compared to the other models. It shows the overall effectiveness and superiority of the proposed security scheme over the other schemes.

TABLE VI. RESPONSE LOSS OF EXISTING AND PROPOSED MODELS

Data Source	BDCA-SDN	IoT-HiTrust	CEF	OSS	Proposed LCCM
20	4.3	4.8	2.5	2	1.8
40	13	8	7	4.5	4.2
60	10	12	10.5	6	5.6
80	14	11.3	13	9	8
100	18	10.5	11.8	7.5	7
120	17	11.5	7.5	8	7.5
140	17.5	13	10	7.5	7
160	17.5	9	11	7.5	7.2
180	15	13	12	6	5.6
200	18	13.5	13	11.5	10.5

V. CONCLUSION

This paper presented a new methodology named as LCCM for enhancing the security of smart city transportation networks. The key contribution of this work is to establish the reliable and valid communication between the V2V and V2I with ensured security and reduced computational complexity. The proposed protocol has been designed based on the operations of symmetric key generation, encryption, and decryption. Before enabling communication, all vehicles, RSUs, mobile devices, sensors, and infrastructure are more required to get registered with its corresponding identity, password, and random number. After that, the authenticity of communicating devices are required to be proved before data transmission or communication. Consequently, the data generation and encryption processes are performed with respect to the random values, identity, and secret keys. Similar to that, the operations like key generation and decryption are performed at the receiver side. This type of communication could efficiently

improve the performance rate with reduced communication cost and time. For validating the performance of the proposed LCCM, various measures such as response loss, average time, response delay, communication cost, and storage overhead have been computed. From the obtained results, it is stated that the proposed LCCM outperforms the other techniques with reduced complexity, cost, and overhead.

REFERENCES

[1] J. Laufs, H. Borrion, and B. Bradford, "Security and the smart city: A systematic review," *Sustainable cities and society*, vol. 55, pp. 102023, 2020.

[2] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Information Systems Frontiers*, pp. 1-22, 2020.

[3] A. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," *Expert Systems*, 2021.

[4] S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi, "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network," *Future generation computer systems*, vol. 112, pp. 724-737, 2020.

[5] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Smart city IoT platform respecting GDPR privacy and security aspects," *IEEE Access*, vol. 8, pp. 23601-23623, 2020.

[6] D. Tokody, A. Albini, L. Ady, Z. Rajnai, and F. Pongrácz, "Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city," *Interdisciplinary Description of Complex Systems: INDECS*, vol. 16, no. 3-A, pp. 384-396, 2018.

[7] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city," *IEEE Access*, vol. 7, pp. 54508-54521, 2019.

[8] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustainable Cities and Society*, vol. 63, pp. 102364, 2020.

[9] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Reports*, vol. 7, pp. 7999-8012, 2021.

[10] X. Li, H. Li, B. Sun, and F. Wang, "Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 4, pp. 2491-2501, 2018.

[11] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794-2830, 2019.

[12] H. Yao, P. Gao, J. Wang, P. Zhang, C. Jiang, and Z. Han, "Capsule network assisted IoT traffic classification mechanism for smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7515-7525, 2019.

[13] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 716-723, 2017.

[14] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4359-4373, 2017.

[15] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433-442, 2020.

[16] S. Kisseleff, W. A. Martins, H. Al-Hraishawi, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surfaces for smart cities: Research challenges and opportunities," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1781-1797, 2020.

[17] A. A. Elsaeidy, N. Jagannath, A. G. Sanchis, A. Jamalipour, and K. S. Munasinghe, "Replay attack detection in smart cities using deep learning," *IEEE Access*, vol. 8, pp. 137825-137837, 2020.

[18] M. A. Jan, W. Zhang, M. Usman, Z. Tan, F. Khan, and E. Luo, "SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application," *Journal of Network and Computer Applications*, vol. 137, pp. 1-10, 2019.

[19] 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 Communications Magazine*, vol. 55, no. 1, pp. 122-129, 2017.

[20] P. K. Sharma, and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650-655, 2018.

[21] M. Saračević, S. Adamović, N. Maček, M. Elhoseny, and S. Sarhan, "Cryptographic keys exchange model for smart city applications," *IET Intelligent Transport Systems*, vol. 14, no. 11, pp. 1456-1464, 2020.

[22] A. K. Mishra, D. Puthal, and A. K. Tripathy, "GraphCrypto: Next generation data security approach towards sustainable smart city building," *Sustainable Cities and Society*, vol. 72, pp. 103056, 2021.

[23] M. Rana, Q. Mamun, and R. Islam, "Current lightweight cryptography protocols in smart city IoT networks: a survey," *arXiv preprint arXiv:2010.00852*, 2020.

[24] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment," *IEEE Access*, vol. 8, pp. 167875-167886, 2020.

[25] D. Wang, J. Shen, J. K. Liu, and K.-K. R. Choo, "Rethinking authentication on smart mobile devices," Hindawi, 2018.

[26] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor

authentication scheme using ECC for wireless sensor networks," *Journal of Network and Computer Applications,* vol. 76, pp. 37-48, 2016.

[27] P. Mohit, R. Amin, and G. Biswas, "Design of authentication protocol for wireless sensor network-based smart vehicular system," *Vehicular Communications,* vol. 9, pp. 64-71, 2017.

[28] H. Lee, D. Kang, J. Ryu, D. Won, H. Kim, and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments," *Journal of Information Security and Applications,* vol. 52, pp. 102494, 2020.

[29] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE transactions on parallel and distributed systems,* vol. 26, no. 4, pp. 938-948, 2014.

[30] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 2, pp. 896-911, 2015.

[31] H. Vasudev, D. Das, and A. V. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Computers & Electrical Engineering,* vol. 82, pp. 106555, 2020.

[32] V. Sharmila, K. Jamuna, K. Jeevitha, I. Kalam, and V. Vennila, "A Novel Authentication Framework with Conditional Privacy Preservation and Non-Repudiation for Fog-Vanet," *Annals of the Romanian Society for Cell Biology,* pp. 8353-8363, 2021.

[33] D. Li, L. Deng, W. Liu, and Q. Su, "Improving communication precision of IoT through behavior-based learning in smart city environment," *Future generation computer systems,* vol. 108, pp. 512-520, 2020.