Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7765994

A NOVEL LIGHTWEIGHT SECURITY MODEL USING DELTA PROBABILISTIC HASHING TECHNIQUE FOR SECURE DATA TRANSMISSION IN IOT

Prasanna Kumar M
Department of Information Science and Engineering, Sri Siddhartha Institute Of Technology, Tumakuru, India, prasan.ctn19@gmail.com

Nalini N
Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bengaluru, India, e-mail: nalini.n@nmit.ac.in

Abstract— The proposed study was primarily concerned with the creation of a lightweight data security model for an IoT data transmission-based application for data transmission and storage in smart cities. The suggested security model's primary contribution is the development of a unique hashing algorithm based on the distinctive pattern of the previous sequential change in value. The Delta Probabilistic Hashing (DPH) based architecture of key extraction technique for data security may do this. Based on the hash key signature approach, this kind of safe data handling procedure provides a random key for data encryption, which may simplify the model and speed up the algorithm's operation. The size of the architecture can be reduced by reducing the number of iterations. This value is the retrieved bit size from the encrypted data. To verify the improvement in our technique, the suggested work is compared to other existing research techniques.

Keywords—Data security, Hashing algorithm, Key generation, Lightweight security

I. INTRODUCTION

Due to the nature of the IoT ecosystem, security is one of the biggest obstacles to IoT implementation and is very difficult. The likelihood of a security breach increases as the type and quantity of connected devices utilized in IoT continue to increase. There is still opportunity to expand the possible attack surfaces for hackers despite the fact that IoT plays a significant role in boosting human welfare and business efficiency. Growing vulnerabilities against data security in the transfer of data, poor software protection, and insufficient authorization are only a few causes for this [1].

Massive volumes of personal data are gathered by real-time IoT applications from corporate transactions in the areas of finance, home, smart lifestyles and healthcare. To access user data, the heterogeneous real-time IoT necessitates the deployment of appropriate security methods. Despite the fact that there are several security methods, they are unable to give the IoT environment higher level security. It is challenging to implement sophisticated data encryption algorithms in IoT devices due to their energy limitations. Therefore, it is necessary for light-weight security algorithms that provide a greater degree of security for IoT data with a low overhead for transmission and processing on these IoT devices [2]. Below is a list of the primary justifications for the requirement of higher level security algorithms.

- Lightweight IoT devices: Because IoT devices are set up with a light operating system, it is impossible to apply security fixes on IoT devices. A lightweight IoT operating system also suffers from a lack of modules to accept and incorporate new programs or libraries.
- Low speed CPU: The Central Processing Units (CPUs) that IoT devices utilize are intended to operate at low speeds and are powered by batteries. As a result, it is more difficult to execute traditional encryption techniques that demand intricate processing [3].
- Heterogeneity of IoT environment: The IoT paradigm includes a variety of wireless protocols, including ZigBee, Z-Wave and Wi-Fi, as well as many device kinds, including computers and RFID tags. The implementation of suitable security solutions is further hampered by this heterogeneous mixture of various devices.
- Low data-rate radio interfaces: IoT devices are accustomed to communicating utilizing low data-rate radio interfaces. Because IoT-based systems employ low bandwidth communication medium, it is challenging to directly implement traditional security mechanisms [4].
- Devices with limited memory: IoT devices often have limited memory. For devices with little memory, there is no security system specifically created.
- Sudden change in network topologies: Because mobile IoT devices are constantly moving, it's possible for them to join or leave a network without any previous preparation. The effectiveness of current security protocols in network topologies is impacted by this nature. Therefore, there are less prospects for these strategies to be applied in the IoT environment [5].

IoT data protection from different security assaults is the main goal of protected IoT. Complex data encryption algorithms are challenging to implement because of the limited capabilities of IoT devices [6]. The majority of customers anticipate being able to access IoT data easily and quickly without having to go through a lengthy verification procedure. Instead of focusing on the devices involved in obtaining IoT data, some authentication methods merely authenticate individuals.

Objectives of this paper are as follows:

- To reduce the limitations of existing techniques related to complexity in data transmission and storage in data security.
- To develop a new technique for data security in the blockchain environment using Delta Probabilistic Hashing (DPH) technique-based architecture.
- To develop a novel lightweight data security with optimal key generation system.
- To analyse the proposed work based on experimentation work and generate better results as compared to other existing methods.

The paper is divided into six main sections. Section I deals with introduction to research work with basic explanation of concepts. Section II is about the related work and to evaluate the review for new proposed work. The section III deals with the explanation of proposed work mainly with the proposed methodology and algorithm. The section IV and V described about the experimentation and results. Last section VI contains conclusion of paper and future recommendations of the proposed work.

II. RELATED WORK

Based on their block size, number of rounds, structures and key size several lightweight cryptographic methods were examined. The security architecture for restricted devices in an IoT context was explored by the authors. [7]

The author of [8] discussed the state-of-the-art in terms of portable cryptographic primitives. In-depth information was provided on the lightweight block cyphers, hash function, stream cyphers, low resource devices and high performance systems.

A novel, lightweight, compact encryption scheme was created by the author in [9] using bit permutation instructions Group Operation (GRP). Using bit permutation instructions, the S-box of PRESENT and the confusion property for GRP were introduced. With regard to both gate equivalents and memory space, the suggested hybrid system produced results that were more compact.

Secure IoT (SIT), a minimal encryption scheme, was suggested by [10]. It offered a simple framework appropriate for an IoT setting. It operated with a 64-bit key and plain text and was a symmetric key block cypher. A 64-bit block cypher was necessary, as well as a 64-bit data encryption key. The design of the suggested algorithm made use of feistel and a mix of substitution-permutation networks.

In [11] author assessed the lightweight symmetric cyphers' hardware and software implementations. The lightweight cyphers were scrutinized based on criteria like cost, speed, efficiency, and balance.

A lightweight block cypher called Hew based on hash functions was presented by [12]. Based on the block cipher FeW the key expansion technique slowed down the FeW hash function's performances. HeW was subjected to security examination against slide attack, rotational distinguisher, differential cryptanalysis, and length extension attack.

It is clear from the aforementioned study that an effective, lightweight, and safe lightweight algorithm is required for data security in the IoT blockchain data context [13], [14], and [15]. The algorithm's implementation aims to improve security system performance in comparison to other conventional security models.

III. PROPOSED WORK

A novel light-weight data security with optimum key generation system is provided for data storage and the transmission process in order to lessen these restrictions and to increase both the performance of data transmission and security. Through a transmission means that transfers the encrypted data, the data is shared with other users. [16] The vast majority of binary sequences that are retrieved from the input data may be used to implement the encryption procedure. [17] In order to recover the functionality of data decryption, this can gather details about the pattern of the signature and the size of the key generation in a sequential procedure. [18]

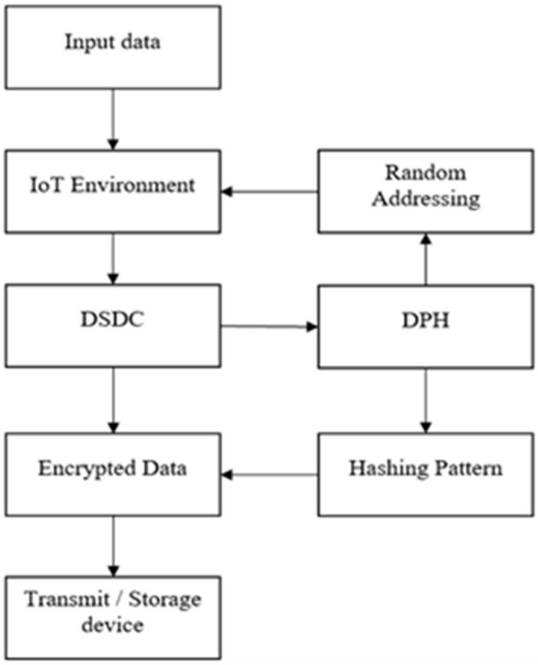

Fig.1: Flow dxiagram of proposed work

For the parameters of error rate, time complexity, and other factors, this suggested work's outcome may be compared to those of current algorithms like ECC, AES, DES and RSA. [19] Last but not least, this can simulate in the data security application to analyse the performance in standard data and then use cutting-edge techniques to validate the outcome of the suggested task. The suggested solution was put into practice using Python scripting, and the performance of the lightweight security system was represented by error rate, throughput, efficient key selection, transmission latency, and other characteristics. [20], [21]

A. Proposed architecture

A lightweight cryptographic system employing DPH and a Double-String Data Cryptographic (DSDC) based encryption and messaging approach is used in the security process. According to this, the DSDC, data encryption is addressed at random using a function-generated key. [22], [23]

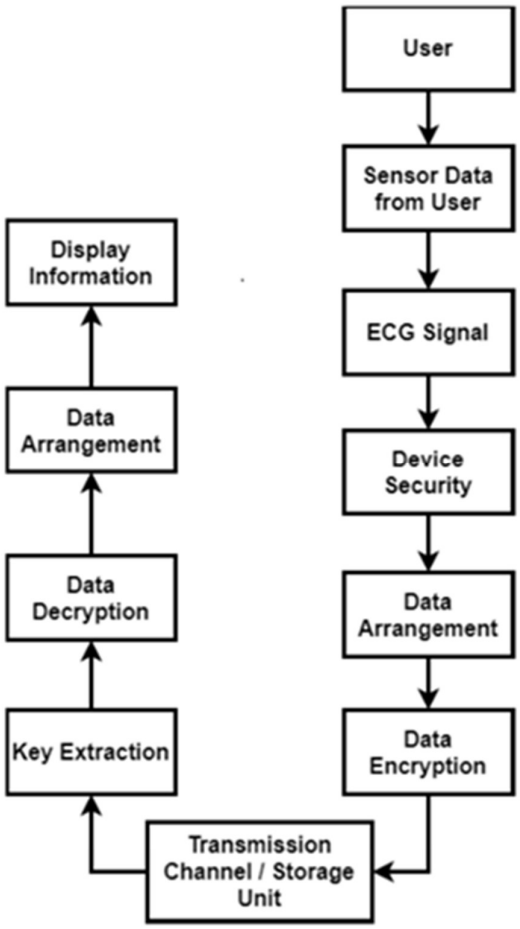

Fig.2: Detailed architecture of proposed model

Due to the ideal key size of the cryptographic approach, the suggested security procedure minimizes the buffer size and has the potential to reduce power consumption. [24] The developed DPH algorithm and combined it with the DSDC in the data security technique. The look-up table of the security model refers to the random key formation, which may produce the public and private key for the security process. [25]

B. Proposed Encryption algorithm

The main intension of this data security algorithm is to optimize the data size with high security model. For this process, the light-weight encryption model was integrated to achieve the high security model with reduced size of data bits. This overall encryption model is depending on the hash key pattern generation block to retrieve the encoded data from the bit stream of data. The architecture of the encryption and the decryption model is shown in figure 3. In that the encoder was divided as two individual blocks to represent the generation of random address and the random key value for the data encoding process. This it refers the generation of private and public key pattern generation for the overall encryption model. The step-by-step procedure with the equation model of IDSE algorithm was presented in the algorithm 1.

Algorithm 1: DSDC based Data Security algorithm

Input: Data samples (D_i)
Output: Encrypted Data (E_D)
Select the random key size as 64-bit chipper (R_b).
Split the data samples into 16-bit block size. This can be represent as the function block f_k.
Construct the data blocks.
Retrieve the $R_{a_i}f_k$ by extracting the 16-bit blocks from (1).
Construct M1, M2, M3, M4 matrix from eqn (2) to (5) based on the block function 'f'.
Estimate the keys as K1, K2, K3, K4 from (6) to (9).
Estimate the key K5 from (10).
Perform the XOR operation to extract the bitwise character '$Y_{o_{i,j}}$' and concatenate encrypted bit sequence from (11).

Let the message can be segment as the blocks which can be represent as in (1).

$$Ra_if_k = f(Rb_if_k) \quad (1)$$

Where,

$$Rb_if_k = \left\| \left(R_{b_{4(j-1)+i}} \right)_{j=1}^{4} \right.$$

To estimate the encryption key pattern, the transformation can be estimate by the random table value that are from the Hexa-decimal value. The table can be represented by the matrixes M1, M2, M3 and M4 respectively. This can be followed by the equation (2) to (6).

$$M1 = \begin{bmatrix} Ra_1f_1 & \dots & Ra_1f_4 \\ \dots & \dots & \dots \\ Ra_1f_{13} & \dots & Ra_1f_{16} \end{bmatrix} \quad (2)$$

$$M2 = \begin{bmatrix} Ra_2f_1 & \dots & Ra_2f_4 \\ \dots & \dots & \dots \\ Ra_2f_{13} & \dots & Ra_2f_{16} \end{bmatrix} \quad (3)$$

$$M3 = \begin{bmatrix} Ra_3f_1 & \dots & Ra_3f_4 \\ \dots & \dots & \dots \\ Ra_3f_{13} & \dots & Ra_3f_{16} \end{bmatrix} \quad (4)$$

$$M4 = \begin{bmatrix} Ra_4f_1 & \dots & Ra_4f_4 \\ \dots & \dots & \dots \\ Ra_4f_{13} & \dots & Ra_4f_{16} \end{bmatrix} \quad (5)$$

The key pattern can be represented by concatenating the bit sequences that are for each block which can be estimated by the equation (6) to (10).

$$K1 = \{\{a_4, \dots a_1\}, \{a_5 \dots a_8\}, \{a_{12} \dots a_9\}, \{a_{13} \dots a_{16}\}\} \quad (6)$$

$$K2 = \{\{b_4, \dots b_1\}, \{b_5 \dots b_8\}, \{b_{12} \dots b_9\}, \{b_{13} \dots b_{16}\}\} \quad (7)$$

$$K3 = \{\{c_4, \dots c_1\}, \{c_5 \dots c_8\}, \{c_{12} \dots c_9\}, \{c_{13} \dots c_{16}\}\} \quad (8)$$

$$K4 = \{\{d_4, \dots d_1\}, \{d_5 \dots d_8\}, \{d_{12} \dots d_9\}, \{d_{13} \dots d_{16}\}\} \quad (9)$$

$$K5 = \bigoplus_{i=1}^{4} K_i \quad (10)$$

From this the ciphered data can be represented as in (11).

$$E_D = \{R_{51}, R_{52}, R_{53}, R_{54}\} \quad (11)$$

Where,

$$R_{o_{i,j}} = \begin{cases} Y_{x_{i,j}} \odot K_i \quad ; \quad j = \{1, 4\} \\ Y_{x_{i,j+1}} \oplus K_i; \quad j = 2 \\ Y_{x_{i,j-1}} \oplus K_i; \quad j = 3 \end{cases}$$

C. Proposed Hashing algorithm

From the cryptographic system, the data security can be defined by the bit size of random key that are initialized for encryption process. The more the size of key size can increase the security level in traditional cryptographic system. This will lead to increasing the data size for storage and transmission process. This may also lead to reduce the throughput of overall system. To overcome, the key pattern are needs to improve and to reduce the size of key with the rate of high security level. This can be achieved by using the light-weight cryptographic system. Compare to the traditional model such as AES, DES, ECC and other types of encryption techniques, the key size was managed and the size was appropriately used according to the properties of data streams that are to transmit over the hash-key structure.

The detailed steps for the DHP based data encryption model was described in the algorithm 2.

Algorithm 2: DPH based Hashing Technique

Input: Data input, D_r
Output: Hash key pattern E_T.
For $i = 1\ to\ n$ **loop**// 'n' is the size of data, T_i in meta-blocks M_v
For $j = 1\ to\ m$ **loop** all resources // Loop running for all the selected resources R_j
Calculate the pattern of key formation, $C_{ij} = D_{ij} + R_j$
Where, R_j – Random weight value for the related parameters of data structure. Ranges from 0->1.
While Key_Bins in Mv **do**
Find the bins of data structure for each data samples with respect to time.

$$T_k = sort(C_i(t))$$

Find the respective key bits to encrypt the data from T_k.

$$Y = min(T_k)$$

Estimate binaries for Y to the random sequence R_j
Make zero's in T_k that are irrelevant to the pattern from M_v
End while
Update R_j
Update C_{ij} for all i
End loop '*j*'
Perform XOR operation to represent the hash key result of overall bit size $E_T(i)$
End loop '*i*'.

IV. RESULT

The results of this paper work is validated based on the parameters that are referring the security level and the rate of complexities that are can be measured from the proposed lightweight security model. The performance of the proposed work can be validated and compared with the existing models that are referred from [26-29]. According to that the proposed model of

data security was developed in the PYTHON (3.8V) script. The overall work was implemented in the blockchain environment with the different data size and its parameters. The table 1 shows the comparison result of proposed lightweight cryptography with the other traditional encryption model. In this table result, the lightweight cryptographic model achieved the better throughput and the efficient key selection that the other traditional model of data security.

Table 1: Comparison table of lightweight method with traditional cryptography methods

Parameters	ECC	DES	AES	Light-weight (Proposed)
Throughput (kb/s)	126	137	114	154
Transmission Delay (ms)	7.94	7.3	8.77	6.49
Error Rate (%)	12.42%	10.58%	7.63%	4.36%
Efficient Key Selection (%)	78.14%	82.57%	88.15%	92.55%
Correlation Coeff.	0.791	0.824	0.867	0.916
Entropy	0.7854	0.8436	0.9287	0.9638

The complexity of the cryptographic algorithm can be expressed by the time and the security level by considering in the both encryption and decryption process. The comparison of the complexity was referred by the parameters of Security (%) and the execution time for both encryption and the decryption process. These comparison is shown in the table 2 and 3. In that, the Packet Delivery Ratio (PDR) and the security (%) states the transmission speed of process and the efficiency of security level for different number of transmission.

Table 2: Comparison table of PDR (%) and the Security (%) for different transmission count

# of Transmission	LWC-DFFF		Proposed	
	PDR (%)	Security (%)	PDR (%)	Security (%)
50	99.2	96.17	99.6	97.24
100	97.8	93.67	98.3	95.15
150	90.2	89.75	93.4	91.27
200	86.26	97.1	89.6	98.53

Table 3: Comparison table of Encryption and Decryption Time (Sec) for different transmission count

# of Transmission	LWC-DFFF		Proposed	
	Enc. time (s)	Dec. time (s)	Enc. time (s)	Dec. time (s)
50	10.06	13.08	9.73	11.2
100	17.88	24.5	16.4	21.7
150	23.07	25.98	20.61	23.83
200	26.68	32.66	25.7	29.5

Further the complexity of algorithm can be described by representation the equation model in terms of processing iteration and the number of functions that includes in the overall result. This was represented in the table 4 and 5 in terms of computation cost and the communication cost respectively. Here, the notations that are used for the cost value estimation can be expressed as

G' - Group in bilinear pair
T_{G_m} – Scalar Multiplication on group G'.
T_{G_a} – Scalar Addition on group G'.
T_{mm} – Modular multiplication in key agreement.
T_h – Hashing function.
T_K – Total Key estimation.
T_{Ra} – Block function.
T_{enc} – Encryption function.
T_{dec} – Decryption function.
$|T|$ – Length of timestamp.
$|ID|$ – Length of Identity.
$Enc(log_q)$ – AES Cipher length of an element.
$Enc(log_b)$ – Proposed Cipher length of an element.

From these comparison of computational cost and the communication cost, the result shows that the proposed model achieved ~1.2% less computational cost and the ~1.6% less communication cost compare to the existing model of Blockchain assisted authentication [27].

$$2T_{G_m} + T_{G_a} + 2T_h + T_{mm} \quad (12)$$
$$2(T_{G_m} + T_{G_a} + T_h) + 2T_{enc} + T_{dec} \quad (13)$$
$$2T_h + T_K + T_{Ra} \quad (14)$$
$$T_{enc} + T_{dec} + 2(T_K + T_{Ra} + T_h) \quad (15)$$

Table 4: Table representation for Computation cost of proposed model compare with [27]

Scenario	Blockchain assisted authentication [27]	Proposed
Message Authentication	Eqn. (12)	Eqn. (14)
Key Agreement	Eqn. (13)	Eqn. (15)

$$|ID| + |T| + log_q \quad (16)$$
$$3|ID| + 2Enc(log_q) \quad (17)$$
$$|ID| + |T| + log_b \quad (18)$$

$|ID| + 2Enc(log_b)$ (19)

Table 5: Table representation for Communication cost of proposed model compare with [27]

Scenario	Blockchain assisted authentication [27]	Proposed
Message Authentication	Eqn. (16)	Eqn. (18)
Key Agreement	Eqn. (17)	Eqn. (19)

This also compared with the functions of structure in terms of time consumption at each stage of existing system from [28] and to the proposed lightweight model. For this, the table 6 represents the execution time for each functions such as the hashing function, encryption, decryption, Cryptographic verification, and point multiplication. Relatively, table 7 shows the comparison result of storage cost in the range of bytes for the existing and proposed model for the same functionalities respectively. The size of data storage is represented in the range of bytes that is to represent the buffer size of the storage / transmission of data to validate the performance of overall functions. This was validated by the key size and the overall byte size of data encryption to store the data.

This was also estimated for the overall execution time (ms) and the storage space (bytes) that is displayed in the graphical representation in figure 3 and 4. The figure 5 shows the comparison of energy consumption in the unit of Joules to compute the encryption and decryption process of proposed and existing model [28].

Table 6: Table comparison of execution time (sec) for proposed with [28]

Functions	ECC-SHA256 [28]	Proposed
Hashing function	0.008	0.007
ECC Enc/Dec function	0.2	0.16
Cryptographic Verification	8.63	4.38
Point multiplication	24	17.4

Table 7: Table comparison of storage cost (bytes) for proposed with [28]

Functions	ECC-SHA256 [28]	Proposed
Hashing function	32	16
ECC Enc/Dec function	32	16
Secret key generation	20	14
Point multiplication	20	14

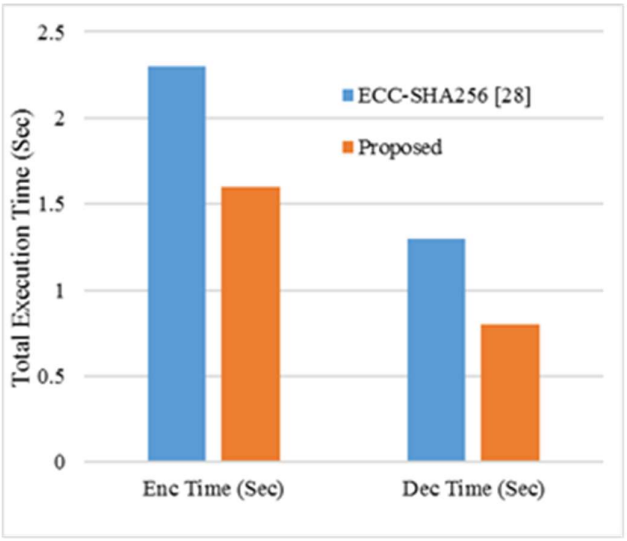

Fig.3: Comparison of Total Execution Time (Sec)

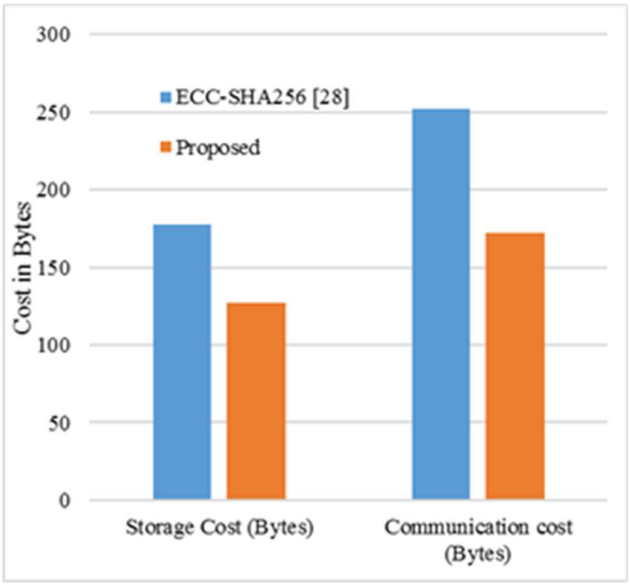

Fig.4: Comparison of Total Execution Time (Sec)

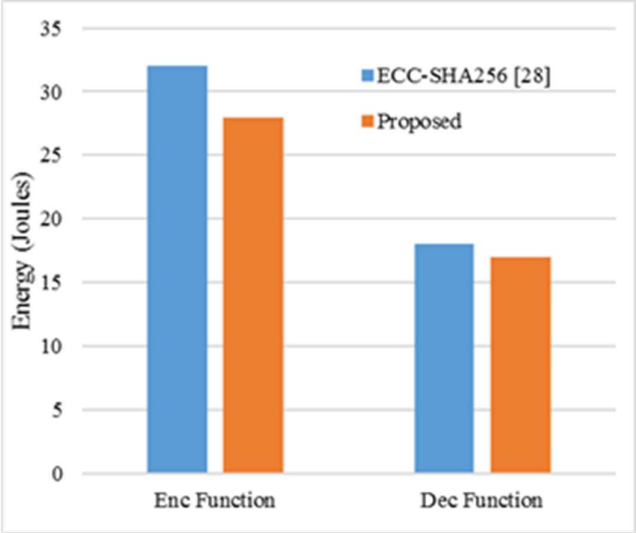

Fig.5: Comparison of Energy consumption (Joules)

These comparison graphs are representing the time, storage cost and the energy consumption of proposed lightweight algorithm is less compare to the existing model of ECC-SHA256 based lightweight cryptographic technique. These measures are estimated for the system configuration of PC with the cycle of process.

To validate the performance of key generation, the time complexity in seconds compare with the existing model of cryptographic technique QBCPDA referred from [29]. This can be represented in the bar plot as shown in the figure 6. Here, the comparison graph shows the execution time for the function of hash estimation and the random key formation in terms of seconds. The proposed achieve the less time consumption than the existing model of QBCPDA.

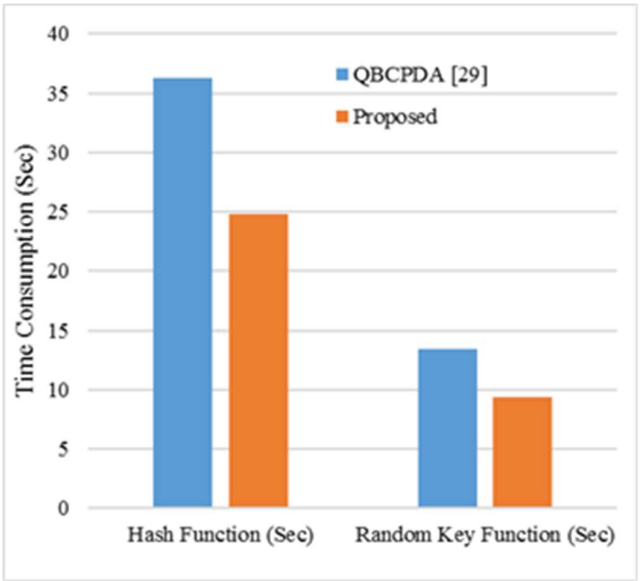

Fig.6: Comparison of time consumption (Sec) in key generation

Result Discussion: As per the comparison table result and the graph representation, the proposed model was validated with the different functions of cryptographic structure and the

different parameters. This validation results are expressed to estimate the performance of proposed lightweight cryptographic model in the blockchain architecture of data storage and the transmission system. The application that are simulated in the blockchain environment are presented to represent the amount of message data that are used to validate the functional modules. According to that, the time consumption, storage range, security level of cryptographic system, energy consumption, transmission time, key size, etc. are calculated and compare with the existing models. From these comparison result, the proposed lightweight cryptographic architecture gains the better result of complexity estimation than the other cryptographic system in the same environment of blockchain. The analytical result proves and justifies the performance of proposed security system in blockchain environment compare to other state-of-art methods and the security system.

V. CONCLUSION

The development of a novel lightweight data security model based on IoT data transmission-based applications for data transmission and storage based on smart city routing was the main emphasis of this work. In this paper a new technique for data security in block chain environment using Delta Probabilistic Hashing (DPH) technique-based architecture is developed with optimal key generation system. The experimentation work confirms the enhancement of proposed model and generate better results as compared to other existing methods. From the above study, it is evident that there is a need for an efficient, lightweight and secured lightweight algorithm for data security in blockchain IoT environment. To lessen the complexity in data transmission and storage limits of current solutions for data security.

For future work some problems related to cost effectiveness and time efficient calculation and comparisons to other existing algorithms can be considered.

ACKNOWLEDGMENT

A heartfelt thanks is conveyed to Professor, College, place, by authors for providing them the mandatory facilities to complete the project effectively.

REFERENCES

[1] Lee I and Lee K, “The Internet of Things (IoT): Applications, investments and challenges for enterprises”, Business Horizons, 2015, pp. 1-10,

[2] M. P. Kumari, T. S. Rao, “A lightweight hybrid scheme for security of big data”, Elsevier Material Science, Technology and Engineering, 2021.

[3] Mahmud Hossain, Ragib Hasan and Anthony Skjellum, “Securing the Internet of Things: A Meta-Study of Challenges, Approaches and Open Problems”, In the proc. of the 37th International Conference on Distributed Computing Systems Workshops, 2017, pp. 220 - 225.

[4] Ali I, S. Sabir and Z. Ullah, “Internet of Things Security, Device Authentication and Access Control: A Review”, International Journal of Computer Science and Information Security, Volume 14, Issue 8, ISSN: 1947-5500, 2016, pp. 456 - 467.

[5] Lin J, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, “A survey on Internet of Things: Architecture, enabling technologies, security and privacy and applications”, IEEE Internet of Things Journal, 2017, pp. 1-17, DOI:10.1109/JIOT.2017.2683200.

[6] H. M. Zeeshan, J. Al-Muhtadi, “Data Security Through Zero-Knowledge Proof and Statistical Fingerprinting in Vehicle-to-Healthcare Everything (V2HX) Communications”, IEEE Transactions on Intelligent Transportation Systems, Vol. 22, No. 6, June 2021.

[7] V. Rao and K. V. Prema, "A review on lightweight cryptography for Internet-of-Things based Applications", Journal of Ambient Intelligence and Humanized Computing, 2020.
[8] S. Singh, P. K. Sharma, S. Y. Moon and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions", Journal of Ambient Intelligent Human Computing, 2017, pp. 1-18, DOI: 10.1007/s12652-017-0494-4.
[9] G. Bansod, N. Raval and N. Pisharoty, "Implementation of a New Lightweight Encryption Design for Embedded Security", IEEE Transactions on Information Forensics and Security, Volume 10, Issue 1, 2015, pp. 142 – 151.
[10] M. Usman, I. Ahmed, M. Imran Aslam, S. Khan and U. Ali Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things", International Journal of Advanced Computer Science and Applications, Volume 8, Issue 1, 2017, pp. 1-10.
[11] J. Hosseinzadeh and Maghsoudhosseinzadeh, "A Comprehensive Survey on Evaluation of Lightweight Symmetric Ciphers: Hardware and Software Implementation", International Journal of Advances in Computer Science, Volume 5, Issue 4, 2016, pp. 31- 41.
[12] M. Kumar, D. Dey, S.K. Pal and A. Panigrahi, "HeW: A Hash Function based on Lightweight Block Cipher FeW", Defence Science Journal, Volume 67, Issue 6, 2017, pp. 636-644, DOI: 10.14429/dsj.67.10791.
[13] Bodeau D, McCollum C, Fox D, "Cyber threat modeling: survey, assessment, and representative framework", The Mitre Corporation, HSSEDI, Bedford,2018.
[14] Mauro Conti, Ali Dehghantanha, Katrin Franke and Steve Watson, "Internet of Things security and forensics: Challenges and opportunities", Future Generation Computer Systems, Volume 78, 2018, pp. 544–546, DOI: 10.1016/j.future.2017.07.060
[15] Lu Weifeng, Ren Zhihao and Xu Jia, "Edge Blockchain Assisted Lightweight Privacy-Preserving Data Aggregation for Smart Grid", IEEE Transactions on Network and Service Management, Vol. 18, No. 2, June 2021.
[16] Mshali H, Lemlouma T and Magoni D, "Adaptive monitoring system for e-health smart homes", International Journal of Pervasive and Mobile Computing, Volume 43, 2018, pp. 1–19,
[17] A. Williams, Beyond 2000: The Rise of Australian Cyber Warfare Capability. New York, NY, USA: Academic, 2020, pp. 549–555.
[18] D. Rayappan and M. Pandiyan, "Lightweight Feistel structure-based hybrid-crypto model for multimedia data security over uncertain cloud environment", Springer Nature 2020, https://doi.org/10.1007/s11276-020-02486-x(0
[19] I. Ahmad and R.-A. Alsemmeari, "Towards improving the intrusion detection through ELM (extreme learning machine)," Comput., Mater. Continua, vol. 65, no. 2, pp. 1097–1111, 2020.
[20] M. Alazab, S. Khan, S. S. R. Krishnan, Q.-V. Pham, M. P. K. Reddy, and T. R. Gadekallu, "A multidirectional LSTM model for predicting the stability of a smart grid," IEEE Access, vol. 8, pp. 85454–85463, 2020.
[21] Fotohi, R., Firoozi Bari, S., & Yusefi, M. (2020). Securing wireless sensor networks against denial-of- sleep attacks using RSA cryptography algorithm and interlock protocol. International Journal of Communication Systems, 33(4), e4234.

[22] Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2017, April). New trust metric for the RPL routing protocol. In 2017 8th International Conference on Information and Communication Systems (ICICS) (pp. 328-335). IEEE.

[23] Zaminkar, M., & Fotohi, R. (2020). SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. Wireless Personal Communications, 114, 1287-1312.

[24] Mohanty, S. N., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. Future Generation Computer Systems, 102, 1027-1037.

[25] Zaminkar, M., Sarkohaki, F., & Fotohi, R. (2021). A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem. International Journal of Communication Systems, 34(3), e4693.

[26] Kumar, K. Vinoth, and D. Balaganesh. "An optimal lightweight cryptography with metaheuristic algorithm for privacy preserving data transmission mechanism and mechanical design in vehicular ad hoc network." Materials Today: Proceedings (2022).

[27] Tan, Yawen, et al. "Blockchain-Assisted Distributed and Lightweight Authentication Service for Industrial Unmanned Aerial Vehicles." IEEE Internet of Things Journal (2022).

[28] Vishwakarma, Lokendra, Ankur Nahar, and Debasis Das. "LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-enabled IoV." IEEE Transactions on Vehicular Technology (2022).

[29] Gupta, Daya Sagar, et al. "Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles." IEEE Transactions on Vehicular Technology 71.3 (2022): 3255-3266.