International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 26 August 2023 **Revised:** 20 October 2023 **Accepted:** 02 November 2023*

A Lightweight Security Model using Delta Probabilistic Hashing Technique for Secured Data Transmission in IoT Systems

Prasanna Kumar M[1], Dr. Nalini N[2]
[1]Research Scholar, Dept. of CSE,
Research Centre, Nitte Meenakshi Institute of Technology,
Bengaluru, India
Visvesvaraya Technological University, Belagavi-590018
email: prasan.ctn19@gmail.com
[2]Professor (CSE) and Dean-Students' Welfare,
Nitte Meenakshi Institute of Technology, Bengaluru, India
Visvesvaraya Technological University, Belagavi-590018
e-mail: nalini.n@nmit.ac.in

Abstract—Secure data transmission is one of the most pressing concerns for resource constrained IoT devices. There is a need for an efficient and lightweight solution for data security in IoT applications. The proposed study is 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 fundamental contribution of the proposed security model is the creation of a distinct hashing algorithm based on the specific pattern of the previous sequential change in value. The Delta Probabilistic Hashing (DPH) based architecture of key extraction technique for data security will perform this. Based on the hash key signature approach, this kind of safe data handling procedure provides a random key for data encryption, which will simplify the model and speed up the algorithm's operation. Our approach's main features are enhanced efficiency and throughput, lightweight data security, and adaptive key generation.

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 the IoT continue to increase. There is still opportunity to expand the possible attack surfaces for hackers, despite the fact that the 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].

The seamless data flow between connected devices, which creates a huge network and enables real-time data monitoring, analysis, and decision-making, is the basis of the Internet of Things (IoT). However, because of its inherent interconnection, the IoT ecosystem is vulnerable to a variety of security risks. Traditional data security methods may not be appropriate for the resource-constrained and diverse IoT landscape since they were created mainly for traditional computer settings. Therefore, it is essential to create cutting-edge security systems that can handle the particular security issues that the IoT presents.

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. Even if there are several security measures, they cannot provide a greater degree of security for the IoT environment. It is challenging to deploy advanced data encryption techniques in IoT devices due to energy restrictions. Therefore, lightweight security methods that provide a higher level of security for IoT data with a reduced transmission and processing cost on these IoT devices are required. [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 the 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 the 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. This heterogeneous combination of diverse devices further complicates the installation of appropriate security measures.

- 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: the 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 consumers want to be able to access IoT data without undergoing a time-consuming authentication process. 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 an innovative lightweight data security with optimal key generation system.
- To analyse the proposed work based on experimentation work and yield better results as compared to other existing methods.

This study is driven by the afore mentioned difficulties and suggests a new lightweight security model to handle the unique security requirements of the Internet of Things. To ensure effective data transmission and protection from any security risks, we try to create a balance between strict data security and the resource limitations of IoT devices.

There are six key sections in the paper. Section I introduce the research effort and provide a foundational explanation of the concepts. In Section II related work is discussed and evaluated the review for new suggested work. The explanation of the proposed study, including the proposed approach and algorithm, is covered in section III. The experimentation and findings were discussed in sections IV and V. Conclusion of the paper and recommendations for further research are found in section VI..

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 methods 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 the 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] which 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], the author assessed the lightweight symmetric ciphers' hardware and software implementations. The lightweight ciphers were mimicked from genetic algorithm [29] in the paper for cost, balance and efficiency. A lightweight block cipher called Hew based on hash functions was presented by [12]. Based on the block cipher FeW, the key expansion technique slowed down the FeW hashes function's performance. HeW was subjected to a security examination against slide attacks, rotational distinguishers, differential cryptanalysis, and length extension attacks. According to the aforementioned study, it is evident that there is a need for an efficient, lightweight, and security algorithm for data security in blockchain IoT environment and to lessen the complexity in data transmission and storage limits of current solutions for data security. [13], [14],[15] and [30].

III. Proposed Work

A novel, lightweight data security system with an optimum key generation system is provided for data storage and the transmission process in order to lessen these restrictions and increase both the performance of data transmission and security. Through a transmission method 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]

The primary focus is on developing a novel security model that optimizes data protection while minimizing the computational burden and power consumption. To achieve this, the research proposes the integration of two key cryptographic techniques - the Delta Probabilistic Hashing (DPH) algorithm and the Double-String Data Cryptographic (DSDC) approach.The DPH algorithm is employed to generate robust hash values for ensuring data integrity. By applying a probabilistic approach, the algorithm detects even slight modifications in the data, enabling the system to identify any tampering attempts effectively. On the other hand, the DSDC technique facilitates data encryption and decryption, ensuring the confidentiality of the information during transmission and storage. By combining these two techniques, the security model achieves a comprehensive and balanced data protection mechanism suitable for resource-constrained IoT devices.

Furthermore, the proposed work introduces the concept of an ideal key size that is carefully selected to match the capabilities of IoT devices. This ensures that the cryptographic approach maintains a high level of security without overburdening the limited resources of these devices. The use of a look-up table for random key formation adds an additional layer of security by providing an efficient means of generating public and private keys. Overall, the proposed security model aims to offer a practical and effective solution for enhancing the security of IoT devices, fostering their widespread adoption and integration in various domains. Through this research, a significant step is taken towards establishing a more secure and efficient IoT ecosystem, thereby enabling the realization of its full potential in revolutionizing modern technology and services.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] The suggested solution has implemented similar transmission approach as per genetic algorithm mentioned in paper [31] and has used its similar solution approach. Fig. 1 shows the proposed work The suggested solution is put into practice using Python scripting, and the performance of the lightweight security system is represented by its error rate, throughput, efficient key selection, transmission latency, and other characteristics. [20]. By presenting a unique, lightweight security model that uses the Delta Probabilistic Hashing (DPH) approach for safe data transmission in the Internet of Things (IoT) environment, the proposed study seeks to overcome the shortcomings of current data security strategies. In contrast to conventional cryptographic techniques, our approach entails developing a unique hashing algorithm[21]. based on the precise pattern of the prior sequential change in value. Our design for key extraction is based on the Delta Probabilistic Hashing (DPH) method, which improves data security while preserving efficiency.

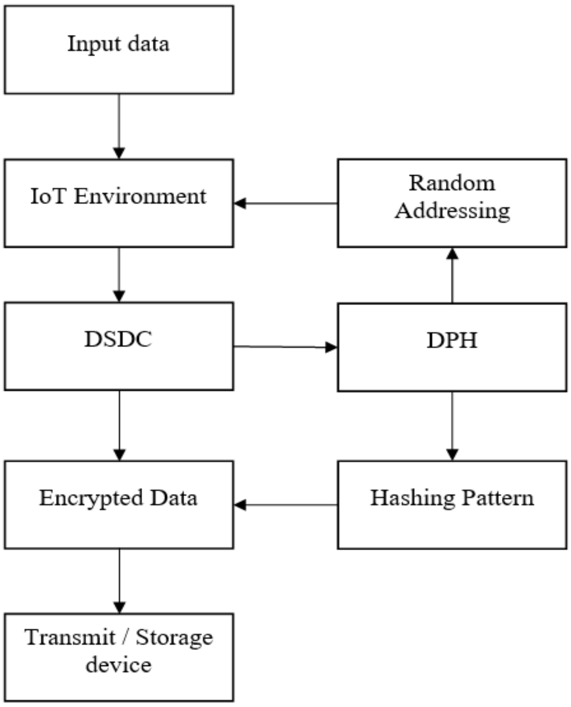

Fig.1: Flow diagram of proposed work

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] Due to the ideal key size of the cryptographic approach, the suggested security procedure minimizes the buffer size and has the potential to minimize 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]

***Article Received:** 26 August 2023 **Revised:** 20 October 2023 **Accepted:** 02 November 2023*

B. Proposed Encryption algorithm

This data security algorithm's primary goal is to reduce data size while maintaining a high level of security. In order to accomplish a high security model with a smaller number of data bits, a lightweight encryption model is included for this process. In order to extract encoded data from a bit stream, this overall encryption system relies on the hash key pattern generating block [32]. The architecture of the encryption and decryption model is shown in Figure 3. To represent the generation of the random address and the random key value for the data encoding operation, the encoder is divided into two separate blocks [33]. In terms of the broader encryption scheme, this relates to the production of private and public key patterns. The IDSE Algorithm is described step-by-step in Algorithm 1 with the equation model.

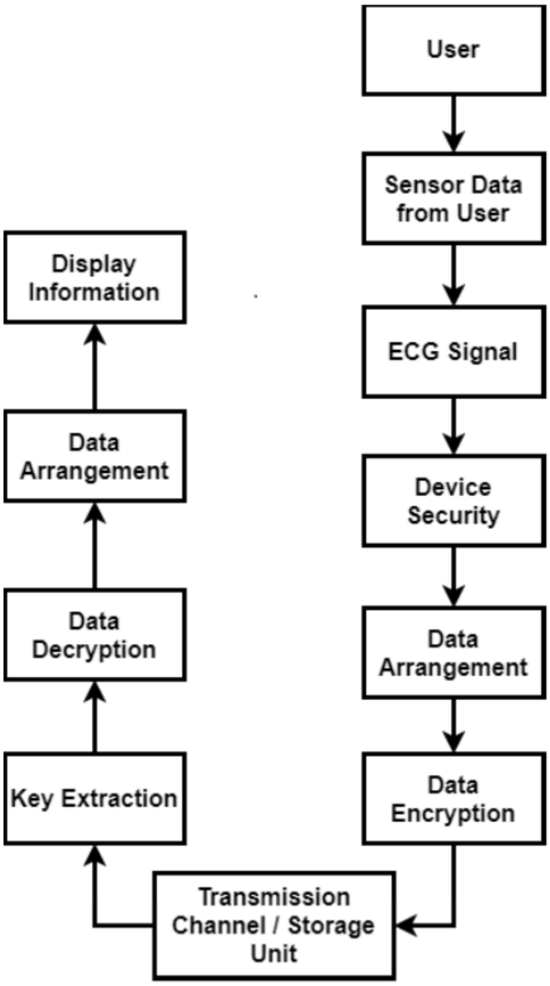

Fig.2: Detailed architecture of proposed model

Algorithm 1: DSDC based Data Security algorithm

Input: Data samples (D_i)
Output: Encrypted Data (E_D)

Choose the 64-bit chipper (R_b) as the random key size.
Divide the data samples into blocks of 16 bits. This can be visualized using the function block f_k.
Build the data chunks.
Extract the 16-bit blocks from (1) and get the R_(a_i) f_k.
Create the M1, M2, M3, and M4 matrices using equations (2) through (5) and the block function "f."
From (6) through (9), assign the keys K1, K2, K3, and K4.
Calculate key K5 using (10).
Extract the bitwise character '$Y_{o_{i,j}}$' using the XOR technique from (11) and concatenate the encrypted bit sequence.

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

$$Ra_i f_k = f(Rb_i f_k) \tag{1}$$

where,

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

The transformation can be estimated using random table values derived from the Hexa-decimal value to determine the encryption key pattern. The matrices M1, M2, M3, and M4 can all be used to represent the table. The equations (2) to (6) will follow this.

$$M1 = \begin{bmatrix} Ra_1 f_1 & \dots & Ra_1 f_4 \\ \dots & \dots & \dots \\ Ra_1 f_{13} & \dots & Ra_1 f_{16} \end{bmatrix} \tag{2}$$

$$M2 = \begin{bmatrix} Ra_2 f_1 & \dots & Ra_2 f_4 \\ \dots & \dots & \dots \\ Ra_2 f_{13} & \dots & Ra_2 f_{16} \end{bmatrix} \tag{3}$$

$$M3 = \begin{bmatrix} Ra_3 f_1 & \dots & Ra_3 f_4 \\ \dots & \dots & \dots \\ Ra_3 f_{13} & \dots & Ra_3 f_{16} \end{bmatrix} \tag{4}$$

$$M4 = \begin{bmatrix} Ra_4 f_1 & \dots & Ra_4 f_4 \\ \dots & \dots & \dots \\ Ra_4 f_{13} & \dots & Ra_4 f_{16} \end{bmatrix} \tag{5}$$

The bit sequences of the block, which may be estimated using equations (6) to (10), are concatenated to create the key pattern.

$$K1 = \{\{a_4, \dots. a_1\}, \{a_5 \dots a_8\}, \{a_{12} \dots a_9\}, \{a_{13} \dots a_{16}\}\} \tag{6}$$

$$K2 = \{\{b_4, \dots. b_1\}, \{b_5 \dots b_8\}, \{b_{12} \dots b_9\}, \{b_{13} \dots b_{16}\}\} \tag{7}$$

$$K3 = \{\{c_4, \dots. c_1\}, \{c_5 \dots c_8\}, \{c_{12} \dots c_9\}, \{c_{13} \dots c_{16}\}\} \tag{8}$$

$$K4 = \{\{d_4, \dots. d_1\}, \{d_5 \dots d_8\}, \{d_{12} \dots d_9\}, \{d_{13} \dots d_{16}\}\} \tag{9}$$

$$K5 = \oplus_{i=1}^{4} K_i \tag{10}$$

The ciphered data can be expressed as in (11) from this.

$$E_D = \{R_{51}, R_{52}, R_{53}, R_{54}\} \tag{11}$$

Where,

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

C. *Proposed Hashing algorithm*

The data security of a cryptographic system can be determined by the initialization bit size of a random key used for encryption. In conventional cryptographic systems, the security level can be increased by increasing the key size. As a result, the amount of data that must be stored and sent will grow. This can also result in a decrease in the system's overall throughput. [33] To overcome, the key pattern must be improved, and the key's size must be decreased while maintaining a high level of security. Utilizing the lightweight cryptographic system will enable this. When compared to the conventional model, which uses encryption methods like AES, DES, ECC, and others, the key size is controlled and used correctly depending on the characteristics of the data streams that will be transmitted across the hash-key structure [34]. To provide a comprehensive understanding of our methodology, we present a detailed architecture and encryption algorithm. Figure 2 illustrates the proposed architecture, highlighting the flow of data through the DPH-based key extraction and the subsequent DSDC-based encryption. The architecture incorporates a look-up table for random key formation, and the retrieved bit size from the encrypted data ensures the optimal key size for enhanced security [35].

To further elaborate on the encryption process, Algorithm 1 outlines the step-by-step procedure for the Double-String Data Cryptographic (DSDC) encryption approach. This algorithm captures the random key generation, bitwise character extraction, and concatenation of encrypted bit sequences [36]. Notably, the DSDC algorithm showcases the efficient key selection process, which is a crucial factor in achieving lightweight data security.

The detailed steps for the DHP based data encryption model is 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// where 'n' is the data size, $T_i$ in meta-blocks equals $M_v$
For $j = 1\ to\ m$ loop all resources // looping for each of the chosen resources $R_j$
    Calculate the pattern of key formation, $C_{ij} = D_{ij} + R_j$
    Where, $R_j$ – is the random weight value for the relevant data structure parameters. runs from 0 through 1.
While Key_Bins in Mv do
        For each data sample, identify the data structure bins 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 '$j$'
   XOR to find the hash key result of overall bit size $E_T(i)$
End loop '$i$'.
```

D. *Flow of the model*

The novelty of our proposed methodology lies in the combination of two key components: the Delta Probabilistic Hashing (DPH) technique and the Double-String Data Cryptographic (DSDC) encryption approach. Unlike conventional cryptographic algorithms that rely on fixed block sizes and complex encryption operations, our approach leverages the unique properties of sequential data changes and random key formation.

1. *Delta Probabilistic Hashing (DPH) Technique:*

Our simple security model is built on the Delta Probabilistic Hashing (DPH) method. The DPH technique generates a hash key signature that speeds up encryption and requires fewer rounds than fixed key sizes since it adjusts dynamically to the pattern of data changes [37]. This significantly reduces the architecture's footprint and makes it possible for IoT devices with limited resources to handle data effectively.

2. *Double-String Data Cryptographic (DSDC) Encryption Approach*:

The proposed encryption technique combines the Double-String Data Cryptographic (DSDC) approach with the DPH approach. The DSDC employs random key generation for data encryption, which enhances system security. By mixing private and public keys, we provide a robust encryption solution that ensures secure data transfer and storage.

E. *Novelty and Benefits of the Proposed Methodology:*

The proposed methodology's novelty lies in its ability to overcome the limitations of existing data security techniques for IoT devices. The key contributions of our approach are as follows:

1. *Lightweight Data Security:*

Our concept dramatically lowers the complexity and resource needs for data security in IoT contexts by employing the Double-String Data Cryptographic (DSDC) method and the Delta Probabilistic Hashing (DPH) technique[38]. Our methodology's ease of integration with IoT devices' slow CPUs, little memory, and low-data-rate radio interfaces is made possible by its minimal weight.

2. *Lightweight Data Security Adaptive Key Generation*

The DPH-based key extraction method generates random keys that improve data encryption by adjusting to the sequential pattern of data changes. By streamlining the encryption process and enhancing security levels, this adaptive key generation lowers processing and transmission costs.

3. *Lightweight Data Security Adaptive Key Generation*
4. *Improved Efficiency and Throughput:*

Our suggested technique shows greater efficiency, higher throughput, and more efficient key selection via testing and comparison with current methods. These results confirm the value of our simple security architecture for securing data storage and transmission in IoT applications. In summary, the suggested methodology addresses the drawbacks of current approaches and ensures increased security and effectiveness while introducing a revolutionary lightweight security model for IoT data transfer[40]. For safe data processing in IoT contexts, the combination of Delta Probabilistic Hashing (DPH) [39] and Double-String Data Cryptographic (DSDC) encryption techniques offers a special and efficient solution. We believe the updated section clarifies the proposed methodology's flow and more persuasively demonstrates how new it is. We would be pleased to include any further recommendations or comments you may have in the study report [41].

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 is developed in the PYTHON (3.8V) script. The overall work is 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 better throughput and the more 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 both encryption and decryption process. The comparison of the complexity is referred by the parameters of Security (%) and the execution time for both encryption and the decryption process. This 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 transmissions.

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 is represented in tables 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 this 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].

$$2T_{G_m} + T_{G_a} + 2T_h + T_{mm} \tag{12}$$

$$2(T_{G_m} + T_{G_a} + T_h) + 2T_{enc} + T_{dec} \tag{13}$$

$$2T_h + T_K + T_{Ra} \tag{14}$$

$$T_{enc} + T_{dec} + 2(T_K + T_{Ra} + T_h) \tag{15}$$

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)

$$|ID| + |T| + log_q \tag{16}$$

$$3|ID| + 2Enc(log_q) \tag{17}$$

$$|ID| + |T| + log_b \tag{18}$$

$$|ID| + 2Enc(log_b) \tag{19}$$

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.

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

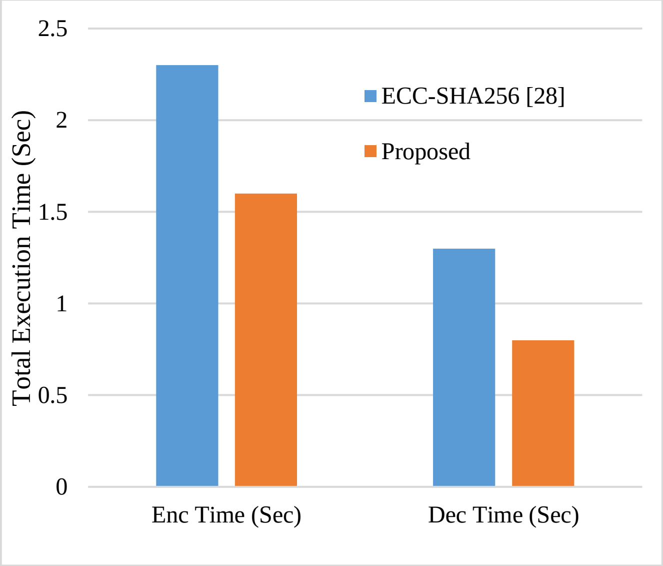

Fig.3: Comparison of Total Execution Time (Sec)

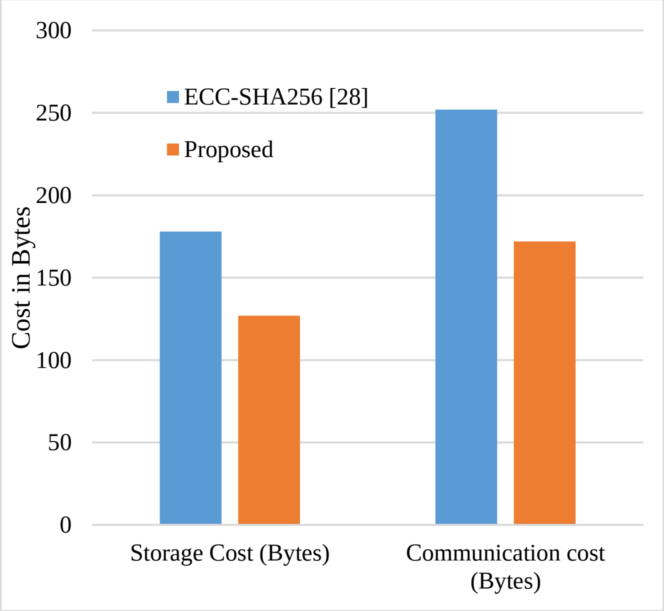

Fig.4: Comparison of Total Execution Time (Sec)

For this, table 6 represents the execution time for each function 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 range of bytes used to represent the buffer size of the storage / transmission of data to validate the performance of overall functions indicates the size of the data storage. This is validated by the key size and the overall byte size of data encryption to store the data.

This is 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. 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].

These comparison graphs represent the time, storage cost and the energy consumption of proposed lightweight algorithm is less compared 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 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 achieves less time consumption than the existing model of QBCPDA.

The comparison graphs clearly illustrate the superiority of the proposed lightweight algorithm over the ECC-SHA256 based approach in terms of time efficiency. The execution time of the proposed algorithm is significantly lower, indicating that it can perform cryptographic operations swiftly without causing any noticeable delays. This attribute is particularly crucial for IoT applications, where devices often need to process a large volume of data in real-time. Another essential aspect is the storage cost, and the proposed lightweight algorithm demonstrates an edge in this regard as well. The amount of memory required to implement the algorithm is considerably less than that of the ECC-SHA256 based technique. By reducing the storage footprint, the proposed algorithm proves to be more compatible with memory restricted IoT devices, allowing them to allocate resources for other essential tasks.

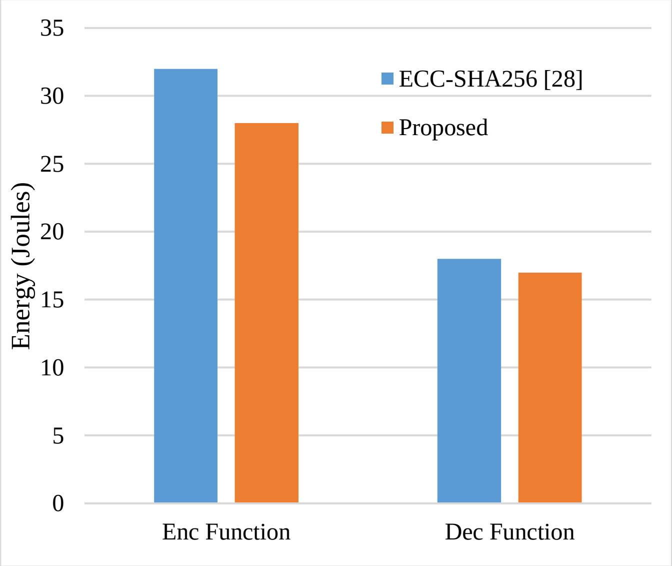

Fig.5: Comparison of Energy consumption (Joules)

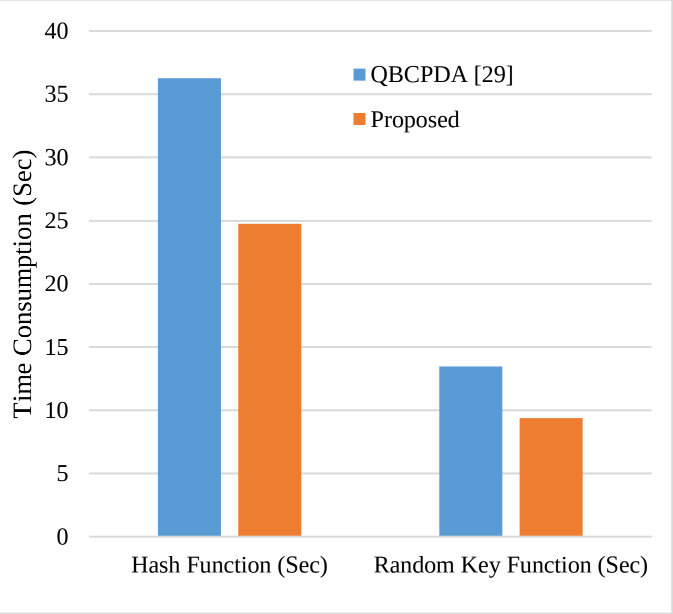

Fig.6: Comparison of time consumption (Sec) in key generation

V. Result Discussion:

As per the comparison table result and the graph representation, the proposed model is validated with the different functions of cryptographic structure and the different parameters. These 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 applications 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 compared with the existing models. From these comparison results. 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 the proposed security system in blockchain environment compared to other state-of-art methods and the security system. The above results were produced in Windows 11, HP pavilion x360 , 11th Generation Core i5 , 2.4 Ghz, 4 Core with RAM of 32 GB.

VI. Conclusion

The development of a novel lightweight data security model in IoT data transmission-based smart city applications for data transmission and storage is 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. Experimentation confirms the improvement of the proposed model, which generates superior outcomes compared to other existing methods. 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 the proposed security system in blockchain environment compared to other state-of-art methods and the security system.

Future research may take into account various issues with the cost and time efficiency calculations and comparisons to other existing algorithms.

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 Maghsoud Hosseinzadeh, “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] Revanna, Jai Keerthy Chowlur, and Nushwan Yousif Baithoon Al-Nakash. "Ant Colony Optimization with Simulated Annealing Algorithm for Google Maps." In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, pp. 320-326. IEEE, 2023.

[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] Revanna, Jai Keerthy Chowlur, and Nushwan Yousif B. Al-Nakash. "Vehicle routing problem with time window constrain using KMeans clustering to obtain the closest customer." Global Journal of Computer Science and Technology 22, no. D1 (2022): 25-37.

[30] 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.

[31] Chowlur Revanna, Jai Keerthy, and Nushwan Yousif B. Al-Nakash. "Tensor Flow Model with Hybrid Optimization Algorithm for Solving Vehicle Routing Problem." In Inventive Systems and Control: Proceedings of ICISC 2023, pp. 113-127. Singapore: Springer Nature Singapore, 2023.

[32] Gopi, R., P. Muthusamy, P. Suresh, C. G. Gabriel Santhosh Kumar, Irina V. Pustokhina, Denis A. Pustokhin, and K. Shankar. "Optimal Confidential Mechanisms in Smart City Healthcare." Computers, Materials & Continua 70, no. 3 (2022).

[33] Rehman, Amjad, Khalid Haseeb, Tanzila Saba, and Hoshang Kolivand. "M-SMDM: a model of security measures using green internet of things with cloud integrated data management for smart cities." Environmental Technology & Innovation 24 (2021): 101802.

[34] D’Andrea, Lucio, Nicolas Sierro, Sonia Ouadi, Tomas Hasing, Elijah Rinaldi, Nikolai V. Ivanov, and Aureliano Bombarely. "Polyploid Nicotiana section Suaveolentes originated by hybridization of two ancestral Nicotiana clades." Frontiers in Plant Science 14 (2023): 999887.

[35] Wang, Jinping, Ruisheng Ran, and Bin Fang. "Global and Local Structure Network for Image Classification." IEEE Access 11 (2023): 27963-27973.

[36] D’Andrea, Lucio, Nicolas Sierro, Sonia Ouadi, Tomas Hasing, Elijah Rinaldi, Nikolai V. Ivanov, and Aureliano Bombarely. "Polyploid Nicotiana section Suaveolentes originated by hybridization of two ancestral Nicotiana clades." Frontiers in Plant Science 14 (2023): 999887.

[37] Gupta, Asmita, Reelina Basu, and Murali Dharan Bashyam. "Assessing the evolution of SARS-CoV-2 lineages and the dynamic associations between nucleotide variations." Access Microbiology 5, no. 7 (2023): 000513-v3.

[38] Matteson, Nathaniel L., Gabriel W. Hassler, Ezra Kurzban, Madison A. Schwab, Sarah A. Perkins, Karthik Gangavarapu, Joshua I. Levy et al. "Genomic surveillance reveals dynamic shifts in the connectivity of COVID-19 epidemics." *medRxiv* (2023): 2023-03.

[39] Revanna, Jai Keerthy Chowlur, Emine Arikan, NandKumar Niture, and Nushwan Yousif B. Al-Nakash. "Advanced Route Optimization using Hybridized Salesforce Geopointe Package." In *ITM Web of Conferences*, vol. 53. EDP Sciences, 2023.

[40] Matteson, Nathaniel L., Gabriel W. Hassler, Ezra Kurzban, Madison A. Schwab, Sarah A. Perkins, Karthik Gangavarapu, Joshua I. Levy et al. "Genomic surveillance reveals dynamic shifts in the connectivity of COVID-19 epidemics." *medRxiv* (2023): 2023-03.

[41] Hemati, Sobhan, Mohammad Hadi Mehdizavareh, Shojaeddin Chenouri, and Hamid R. Tizhoosh. "A non-alternating graph hashing algorithm for large-scale image search." *Computer Vision and Image Understanding* 219 (2022): 103415.