Vol.67: e24231193, 2024
https://doi.org/10.1590/1678-4324-2024231193
ISSN 1678-4324 Online Edition

BABT
Brazilian Archives of Biology and Technology

Article - Engineering, Technology and Techniques

An Improved Lightning Search Algorithm-based End-to-End Lightweight Partially Homomorphic Encryption Approach for Enhanced IoT Security

Sarmila Kalamani Balasubramanian[1*]
https://orcid.org/0009-0000-1591-273X

Manisekaran Sulur Velusamy[2]
https://orcid.org/0000-0001-6883-7470

[1]Sri Eshwar College of Engineering, Department of CSE, Coimbatore, Tamil Nadu, India; [2]Anna University Regional Campus, Department of IT, Coimbatore, Tamil Nadu, India.

Editor-in-Chief: Alexandre Rasi Aoki
Associate Editor: Alexandre Rasi Aoki

Received: 08-Dec-2023; Accepted: 15-Apr-2024.

*Correspondence:kbsarmilacse@gmail.com; (S.K.B.).

HIGHLIGHTS

- ILSA-LPHEA for Securing the IoT Environment.
- For securing the data in the IoT environment, a lightweight partially homomorphic encryption (PHE) approach is used
- Enhancing privacy, confidentiality, and authentication, enabling end-to-end encryption.

Abstract: The Internet of Things (IoT) security is a highly challenging research domain. The IoT user devices frequently function in vulnerable platforms that cause many security problems that can be considered. The model lightweight cryptographic (LWC) method stake place to reflect the importance of cryptographic systems which offer safety with the employ of an effectual count of resources. The purpose of the lightweight system's design is to strike a balance in many features like low resource demand, performance, and cryptographic algorithm stability and strength. Therefore, this study develops a new Improved Lightning Search Algorithm based End-to-End Lightweight Partially Homomorphic Encryption Approach (ILSA-LPHEA) for Securing the IoT Environment. For securing the data in the IoT environment, a lightweight partially homomorphic encryption (PHE) approach is used. Since key generation remains an important process to establish secure data transmission among IoT devices and servers, the ILSA is used. The hybridization of lightweight encryption with PHE strategy provides better security by enhancing privacy, confidentiality, and authentication, enabling end-to-end encryption. A detailed experimental result analysis highlighted the better solution of the ILSA-LPHEA algorithm with recent models.

Keywords: Internet of Things; Security; Lightweight cryptography; Partial homomorphic encryption; Key generation.

INTRODUCTION

According to the development and extensive usage of Internet of Things (IoT) applications with the arrival of IoT and cloud computing (CC), wireless communication and mobile technologies have become significant notations. IoT targets to offer connectivity for whatever with the least computing abilities and storage [1]. Security is a key challenge in cloud-incorporated IoT, and the user information stored in the cloud needs secure protection. Subsequently, resource-limited devices have insufficient power (battery) supply and lower computing ability because of these confines [2]; it is difficult to perform standard cryptographic primitives on these smaller devices. Additionally, these smaller computing devices are not executed well while standard cryptographic measures have been implemented for these lightweight devices [3].

Traditionally encryption can be a kind of cryptography whereby the receiver and transmitter both employ a similar key for encrypting and decoding data. This can be the only category of encryption in utilization until public key encryption has been constituted [4]. An intruder may attack the computer system or network and make it impracticable. Protecting privacy in IoT nodes is difficult because of numerous factors [5]. Primarily, the CPU in IoT devices is decreased and does not calculate complex methods. Secondarily, the power consumption of the security method must be lower because most IoT devices function with a battery [6]. Figure 1 illustrates the structure of security in an IoT network.

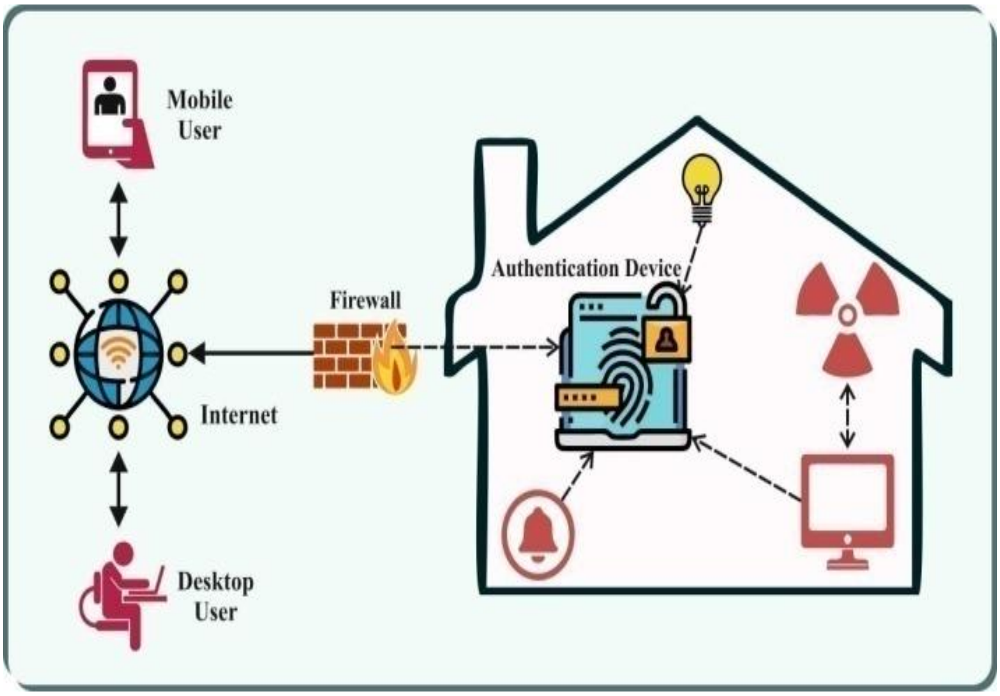

Figure 1. Security in IoT network

Then, modest sensors have been interconnected to hide massive physical networks. Lastly, the expenses of applying the security method must be small to employ as many devices as possible. Standard cyber security cryptography namely blowfish, RC6, DES (Data Encryption Standard), RSA (Rivest-Shamir-Adleman), and AES (Advanced Encryption Standard) could not be employed promptly in these smart fields owing to the dynamic aspects of smart cities, scalability, and heterogeneity [7]. RC2 technique consumes more power, with the contrary blowfish in the minimum one. Further, the majority of these methods consumed larger power when functioning. Biswas is compared with numerous WSN sensor nodes and establishes those resource-limited devices, which can be the lowest possible two kilobytes (kB) and one kB of Electrically Erasable Programmable Read-Only Memory (EEPROM) and Random Access Memory (RAM) respectively. These sensors could not employ the resource-limited standard security techniques [8].

Therefore, safe communication is the most important issue in lossy and lower power systems which certainly describe the requirement for developing Lightweight Cryptographic (LWC) methods for IoT security. Cryptography is not assured higher accessibility, a major key element of data security. It stimulates research workers to determine cryptographic primitives, which is acceptably performed with these widespread smaller devices. Therefore, LWC has been a developing field of cryptography in recent years that could be usually described for resource-limited devices [9]. The LWC is primarily applied for smaller devices even today, LWC aims to be a highly extensive type of device. It involves the development and study of cryptographic primitives for resource-limited devices [10]. This can be a hybrid of two domains namely hardware and cryptography technologies.

This study develops a new Improved Lightning Search Algorithm based End-to-End Lightweight Partially Homomorphic Encryption Approach (ILSA-LPHEA) for Securing IoT Environment. For securing the data in the IoT environment, a lightweight partially homomorphic encryption (PHE) approach is used. With the application of ILSA, the optimal key generation process can be accomplished and it is significantly less resource-intensive. The hybridization of lightweight encryption with PHE strategy provides better security by enhancing privacy, confidentiality, and authentication, enabling end-to-end encryption. A detailed experimental result analysis highlighted the better solution of the ILSA-LPHEA approach with recent models.

RELATED WORKS

In [11], a security technique for protecting IoT networks, and processes from memory heap penetration and overcoming adaptation threats was developed. This presented approach avoids engaged attacks by encoding the object Garbage Collection in the execution period. For making an exceptional signature method, the Cryptographic Hash Function (CHF) utilizes a precise one-way hash method. This introduced model employs a one-time Key (OTK) and L-function-enabled ECC for protecting the memory heap. The authors [12] introduced a novel BC-Enabled Shark Smell Optimizer with Hopfield Chaotic-NN (SSO-HCNN) to protect encoding across the IoT platform. This developed SSO-HCNN method employs a complex Chaotic Map (CM) that could be incorporated into tent and staged logistic maps for firstly processing the images and then, developing the variables required in Arnold mapping. Also, the SSO method could be proposed under higher PSNR and coefficient FF for choosing the best secret and public keys of the model between the random numbers.

In [13], a resource-effective endwise security system was designed by offloading computations and storing security factors to fog nodes from the proximity. The exploration exhibits developed method exceeds Transport Layer Security (TLS) at resource utilization whereas this can preserve equivalent authenticate endwise communication among interconnecting IoT devices. A slime mold optimizer with ElGamal Encryption with Hybrid DL-assisted Classification (SMOEGE-HDL) method fromthe IoT platform. In the primary phase, the SMOEGE algorithm was implemented for encrypting the information from the IoT platforms. The SMO method was exploited for enhancing key generation in the EGE approach.

A Lightweight Security Algorithm (LSA) as a hybrid technique produced by incorporating the Security Protocol for Sensor Networks (SPINS) at the Secure IoT (SIT) encrypted system for enhancing WSN's information security whereas lessening the threshold of threats as well as reducing energy consumption in WSNs with not affecting the effectiveness of networks. A Fully Homomorphic Encryption with Optimum Key Generation Secure Group Communication (FHEOKG-SGC) approach in the IoT infrastructure. To achieve this, this introduced FHEOKG-SGC algorithm first develops an FHE-assisted encryption method for protecting the information at the IoT platform. Then, the keys in the FHE approach have been optimum selected employing the SCA. Simultaneously, the plum tree algorithm (PTA) was implemented to identify the routes at the IoT network.

A lightweight encryption method for IoT devices, which can be developed to offer a balance between resource proficiency and security. The Sym-BRLE (Binary Ring-Learning encryption) method is dependent upon the BRLE with an error encryption technique, which must be developed for increasing polynomial multiplication evaluation and random number selection for satisfying IoT system needs. The BC-assisted IoT platforms. Firstly, the medical images are taken of the patients through IoT devices. Subsequently, the obtained images could be encoded utilizing a signcryption algorithm. Besides, the optimum key generation process has been implemented via the WDOA technique to enrich the effectiveness of this method.

THE PROPOSED MODEL

In this study, we have developed and designed a novel ILSA-LPHEA technique for the security IoT environment via the LWC process. For securing the data from the IoT platform, the ILSA-LPHEA approach makes use of the PHE approach. In addition, ILSA is used for optimal key generation, which enables to establishment of secure data transmission among the IoT devices and servers, the ILSA is used. Figure 2 represents the entire procedure of ILSA-LPHEA approach.

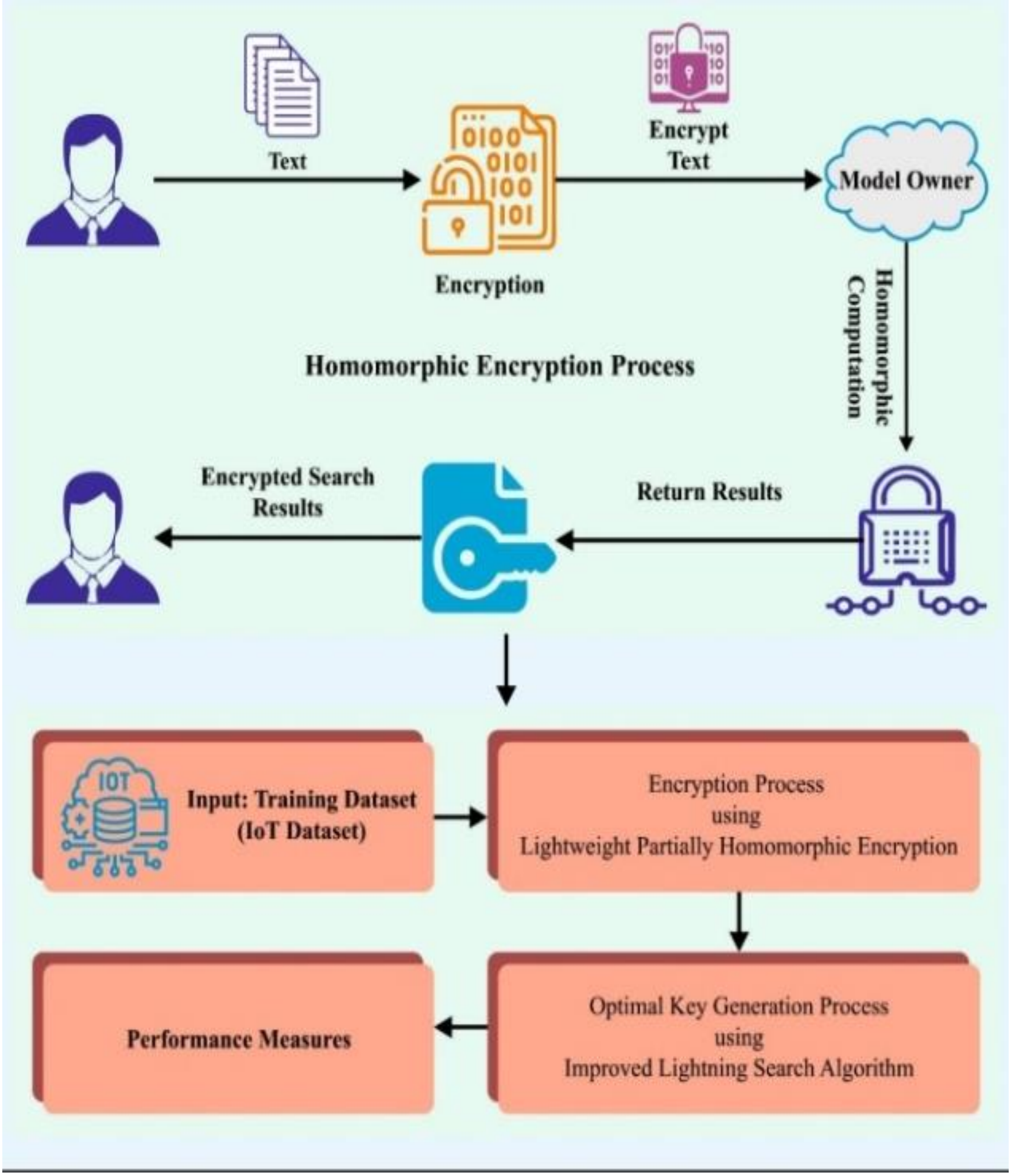
Text
Encrypt Text
Model Owner
Encryption
Homomorphic Encryption Process
Homomorphic Computation
Encrypted Search Results
Return Results
IOT
Input: Training Dataset (IoT Dataset)
Encryption Process using Lightweight Partially Homomorphic Encryption
Performance Measures
Optimal Key Generation Process using Improved Lightning Search Algorithm

Figure 2. Overall process of ILSA-LPHEA approach

Encryption Process

The communication condition in homomorphic encryption is the user's need to execute computational functions with unreliable outsourcing [19]. The user initially utilizes a function that permits functions that execute on encrypt values. Next, it takes to encode the input values previously sent and decode the cloud outcome. The user needs to calculate the performance of $\alpha\theta\beta$, challenging untrusted providers and insecure channels. Eq. (1) has been employed to betterthe security level of systems and attain dependableoutcomes. Butψrefers to the ciphertext, πimplies the plaintext, $k$stands for the confidential key, and $r$implies thearbitrary number.

$$\psi=(\pi\times k+r\times p)\mathrm{mod}n \tag{1}$$

Assume that the plaintext $m$is a group of decimal digits and individuallycontrolall the digitsm_i whereas$0 \leq m_i \leq 9$. Lastly, it multipliesall the digitsm_i by secretkey sk_i. The utilization of public keys (pk_i) is provided as the asymmetric form of this method, and it can be appropriate to observe that $k_i$is smaller.

For construction:

$$\text{KeyGen: } (pk_i,sk_i) \text{ is equivalent}((k_i+r_i\times p,n), (k_i, p))$$

$$Enc(m)\text{: } c=m_0\times pk_0+m_1\times pk_1+\ldots m_i\times pk_i\text{, where } pk_i < pk_{i+1}$$

$$\text{Dec(c):}m=\Sigma_{i=l}^{0}(\frac{c}{k_i})\times 10^i, c\leftarrow c-c\times k_i\text{, with } \left(\frac{c}{k_i}\right) \text{ presents the quotient of } c\div k_i.$$

As demonstrated in Algorithm 1, if $m = m_j m_{j-1} \ldots m_0$ with $m_0$implies the co-efficient of 10^0,$m_i \in \{0, \ldots, 9\} \forall i \in \{0, \ldots, j\}$, and $m_j \neq 0$.

$$c=m_0\times pk_0+m_1\times pk_1+\ldots m_j\times pk_j \text{so}=m_0\times(k_0+r_0\times p)+m_1\times(k_1+r_1\times p)+\ldots m_i\times(k_j+r_j\times p).$$

We get:

$$c=\left(m_0\times k_0+m_1\times k_1+\ldots m_j\times k_j+r\times p\right)\text{mod} n \tag{2}$$

with$r=m_0\times r_0+m_1\times r_1+\ldots m_i\times r_j$.

Observing that: $m_0\times k_0+m_1\times k_1+\ldots m_j\times k_j<p$.

The mod n refers to the modulus operation, where "n" is a positive integer.

Key Generation Process

With the application of ILSA, the optimum key generation procedure has been accomplished and makes it significantly less resource-intensive. The LSA is inspired by the natural phenomenon of lightning [20]. Once the lightning can be produced, a "discharger" body of particles from the air is formed that is quickly moved by the atmosphere, forming a stepped leader and initial particle channel through the collisions between particles. Lightning is random and predictable regarding where it reaches the ground due to its tortuous and probabilistic nature of lightning. It is noted that the discharger body produces a particle channel through collision, which forms a stepped leader. Related to the concept of individual from the population in the differential evolution (DE) model, the concept of "discharger" is considered a set of solution candidates in the optimization problems. The mathematical modelling of stochastic distribution function has been developed for resolving the optimizer problems based on three kinds of dischargers namely spatial, stepped leader, and transitional dischargers.

In the earlier phase, the discharger quickly passes through the air and loses energy once it collides with other atoms and molecules from the air. Once the discharger follows a longer path, it cannot explore or ionize the large space, however, it only ionizes particles within smaller surrounding space. During the LSA, the energy of the discharger has been utilized for controlling the local and global search spaces.

The dischargers are bifurcated in two different ways as lightning falls onto the ground. The initial kind of bifurcation forms two symmetrical channels, as follows.

$$\overline{p}_i=a+b-p_i \tag{3}$$

In Eq. (3), the up and low boundaries of the search space are $a$and b, and the original and symmetric channels designed through bifurcation are p_i and $\overline{p}_i$ correspondingly. The energy of both channels was compared, for maintaining a fixed size of population, and one channel hasbeen taken.

The next type removes the worse channel. The process repeatedly improves the channel time. The worse channel can be removed. The optimum channel value has been allocated to the worse channel for maintaining a fixed-size population, and the channel time was reset. Figure 3 depicts the steps involved in LSA. By inspiring the discharge processes of stepped leader, transitional, and spatial dischargers, the LSA can be evaluated:

Transitional discharger

This discharger is used to create the population initialization that randomly broadcasts downward in the thundercloud. Hence, it follows a standard distribution, and its density probability function is formulated by:

$$f\left(x^{T}\right)=\begin{cases}\frac{1}{b\text{-}a} a\leq x^{T}\leq b\\ 0 \quad x^{T}<a or x^{T}>b\end{cases} \tag{4}$$

In Eq. (4), a group of candidate solutions isx^T and the up as well as low boundaries of the solution space are a and b, correspondingly

Spatial discharger

This discharger tries to obtain the optimum location of the stepped leader. Using an exponential distribution, its location can be modelled,

$$f\left(x^{T}\right)=\begin{cases}\frac{e^{-x^{2}/\mu}}{\mu} & x^{s}\geq 0\\ 0 & x^{s}\leq 0\end{cases} \tag{5}$$

In Eq. (5), a group of candidate outcomes is $x^s$and the shape parameterμ controls the direction of next iteration is formulated by:

$$p^{s}_{i\_new}=p^{S}_{i}\pm e^{rand(\mu_{i})} \tag{6}$$

In Eq. (6), the random integer is$e^{rand(\mu_i)}$, and the distance between the spatial discharger p^S_i and stepped leader discharger p^L isμ_i. The p^S_i is updated to position $p^s_{i\_new}$ if the energy $E^s_{i\_new}$ of novel spatial discharger $p^s_{i\_new}$ is larger than the energy E^S_i of new spatial discharger p^S_i. Or else, p^S_iremain the same until the next update.

Stepped leader discharger

Using uniform distribution, this discharger is modelled with the density probability function as follows:

$$f(x^L)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(xL-\mu)^2}{2\sigma^2}} \tag{7}$$

In Eq. (7), the shape and scale parameters are σ and μ, which reflect the mining capacity at the existing position. In this phase, σ exponentially reduces as the discharger gets closer to the ground. In the next iteration, the direction of stepped leader discharger p^L can be given as

$$p^{L}_{new}=p^{L}+normrand\left(\mu^{L},\sigma^{L}\right) \tag{8}$$

In Eq. (8), $normrand\left(\mu^{L}, \sigma^{L}\right)$ is a random integer from the uniform distribution. The p^L is updated to take location p^L_{new} if the energy E^L_{new} of novel stepped leader discharger p^L_{new} is higher than the energy E^L of originally stepped leader discharger p^L. Or else, p^L remains the same until the next update is performed.

The ILSA is derived by integrating the LSA with the chaotic initialization. The term "chaotic" refers to an irregularly distributed system. Chaotic searching is represented by ergodicity, non-linearity, initial-value sensitivity, and randomness features that enhance the search performance of the algorithm. Chaotic mapping method includes tent mapping, logistic mapping, Lozi mapping, cubic mapping, and Chebyshev mapping. The chaotic tent mapping used for initializing the population can efficiently enhance the population diversity, such that the initial solution is uniformly distributed from the solution space. We used tent map to create a chaotic sequence as follows:

$$x_{n+1}=f(x_{n})=\begin{cases}\frac{x_{n}}{\alpha}, x_{n} e[0,\alpha]\\ \frac{1-x_{n}}{1-\alpha}, x_{n} e[\alpha, 1]\end{cases} \tag{9}$$

Where∈(0,1). Then, the chaotic sequence map towards the solution space of the problem:

(1) Based on Eq. (9), nm-dimension individuals are produced, α=0.49, and the meta-individuals are $=(x_1,x_2, \ldots,x_m),x_i\in(0,1),i=1\ldots,m,x_i\in(0,1)$, and i=1,2,…,m.

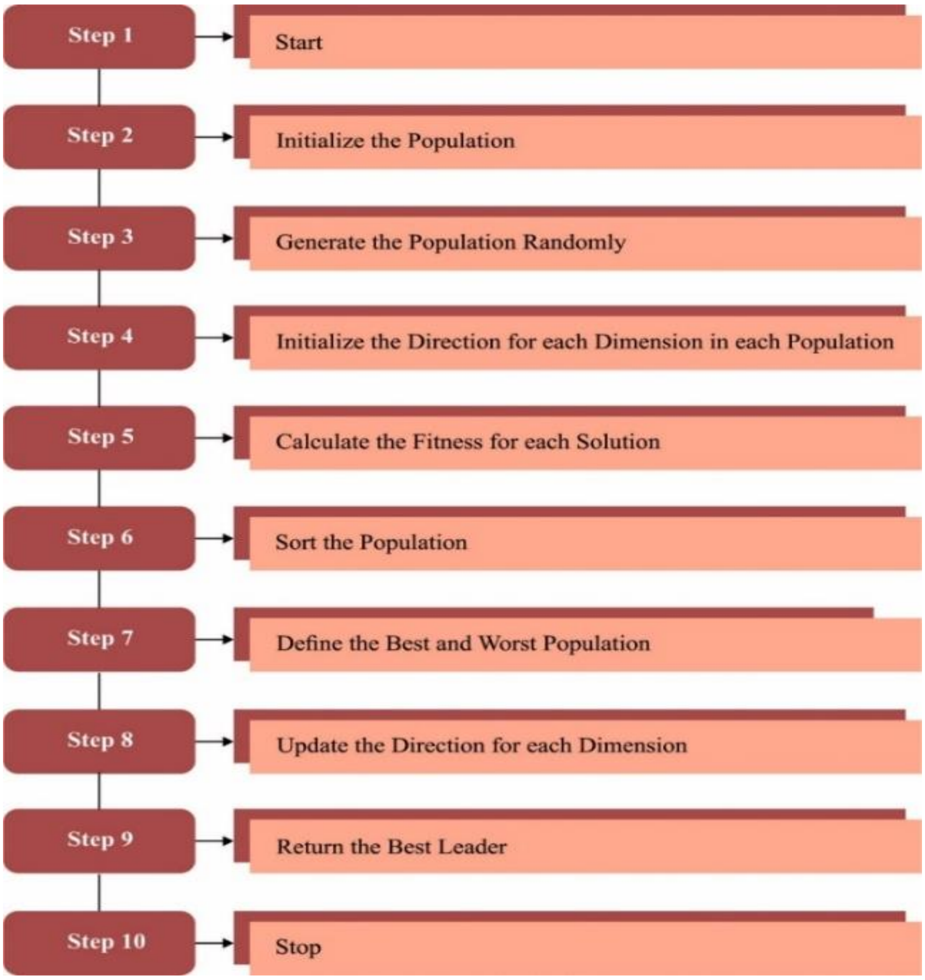
Step 1
Start
Step 2
Initialize the Population
Step 3
Generate the Population Randomly
Step 4
Initialize the Direction for each Dimension in each Population
Step 5
Calculate the Fitness for each Solution
Step 6
Sort the Population
Step 7
Define the Best and Worst Population
Step 8
Update the Direction for each Dimension
Step 9
Return the Best Leader
Step 10
Stop

Figure 3. Steps involved in LSA

A primary population has been attained by mapping the meta-individual to search space:

$$y_i=a_i+x_i\times(b_i-a_i) \qquad (10)$$

In Eq. (10), the next and prior terms in the space area$_i$ and b$_i$, correspondingly, the value of meta-and primary solution individuals in i^{th} dimension space isx$_i$, and y$_i$.

```
# Lightning Search Algorithm (LSA) with Chaotic Initialization
# Initialize parameters
a, b = lower and upper boundaries of the search space
population_size = fixed size of the population
max_iterations = maximum number of iterations
# Chaotic initialization using tent map
function chaotic_initialization(alpha, m):
  initialize empty array meta_individuals
  for i in range(m):
x_i = random value in the range [0, 1]
    apply tent map to x_i based on Eq. (5.9)
    append result to meta_individuals
  return meta_individuals
# Map meta-individuals to search space
function map_to_search_space(meta_individuals, a, b):
  initialize empty array primary_population
  for x_i in meta_individuals:
y_i = a + x_i * (b - a)  # based on Eq. (5.10)
    append y_i to primary_population
  return primary_population
# Lightning Search Algorithm (LSA)
```

```
    function LSA(initial_population, max_iterations):
    current_population = initial_population
        for iteration in range(max_iterations):
            # Evaluate and update population based on lightning-inspired dischargers
            update_population_based_on_transitional_discharger(current_population)
            update_population_based_on_spatial_discharger(current_population)
            update_population_based_on_stepped_leader_discharger(current_population)
            # Remove worse channel and reset channel time
    remove_worse_channel(current_population)
     # Optional: Evaluate and update population based on other optimization criteria
return best_solution_in_current_population
```

Decryption Process

To develop a new digits of plaintext$m$in the cipher textc, the final part rxp can beremoved by calculating the modulo function. Afterward, reducing i, ccan be separated consecutively on k_i. At last, the attained digits are multiplied successively by 10^i (reducing i).

Lemma1. *If*$\frac{c}{k_i}=m_i \Rightarrow Dec(c)=m$.

Proof. Lemma1 $\Leftrightarrow m_0 \times k_0+m_1 \times k_1+\ldots m_{j-1} \times k_{j-1}<m_j \times k_j \forall m_i 0 \leq m_i \leq 9$,

that is $\frac{m_0 \times k_0+m_1 \times k_1+\ldots m_{i-1} \times k_{i-1}}{k_i}=0$.

RESULTS AND DISCUSSION

In this section, the security analysis of the ILSA-LPHEA technique is examined under distinct key sizes and file sizes. In Table 1, the encryption time (ET) and decryption time (DT) results of the ILSA-LPHEA technique with recent models are made under key size of 48b [21].In Figure 4, the comparative ET results of the ILSA-LPHEA technique under key size of 48b is given. The figure shows that the XTEA and XXTEA models have reported higher ET values. At the same time, the TEA and NTSA models have reported slightly decreased ET values. But the ILSA-LPHEA technique exhibits better performance with the least ET of 0.389ms, 0.509ms, 0.945ms, 0.994ms, 1.095ms, 1.705ms, and 1.959ms, under file size of 1.6KB to 26.7KB, respectively. In Figure 5, a detailed DT result of the ILSA-LPHEA technique is compared with other encryption models with a key size of 48b.

Table 1. ET and DT outcome of ILSA-LPHEA algorithm with other methods underkey size of 48b

Key size : 48b					
FILE SIZE (KB)	ENCRYPTION Time (ms)				
	TEA Model	XTEA Model	XXTEA Model	NTSA Model	ILSA-LPHEA
1.6	0.389	0.628	0.435	0.377	0.154
2.6	0.509	0.852	0.606	0.454	0.245
6.8	0.945	1.544	1.924	0.714	0.516
8.6	0.994	2.281	1.364	0.964	0.762
12.2	1.095	2.459	1.535	1.030	0.810
16.2	1.705	3.905	2.145	1.375	1.194
26.7	1.959	4.328	2.873	1.756	1.572
DECRYPTION Time (ms)					
1.6	0.377	0.630	0.409	0.374	0.181
2.6	0.510	0.843	0.550	0.481	0.296
6.8	0.903	1.548	1.907	0.811	0.595
8.6	0.985	2.257	1.338	0.965	0.754
12.2	1.070	2.386	1.533	1.057	0.841
16.2	1.701	3.858	2.129	1.403	1.211
26.7	1.948	4.416	2.961	1.802	1.599

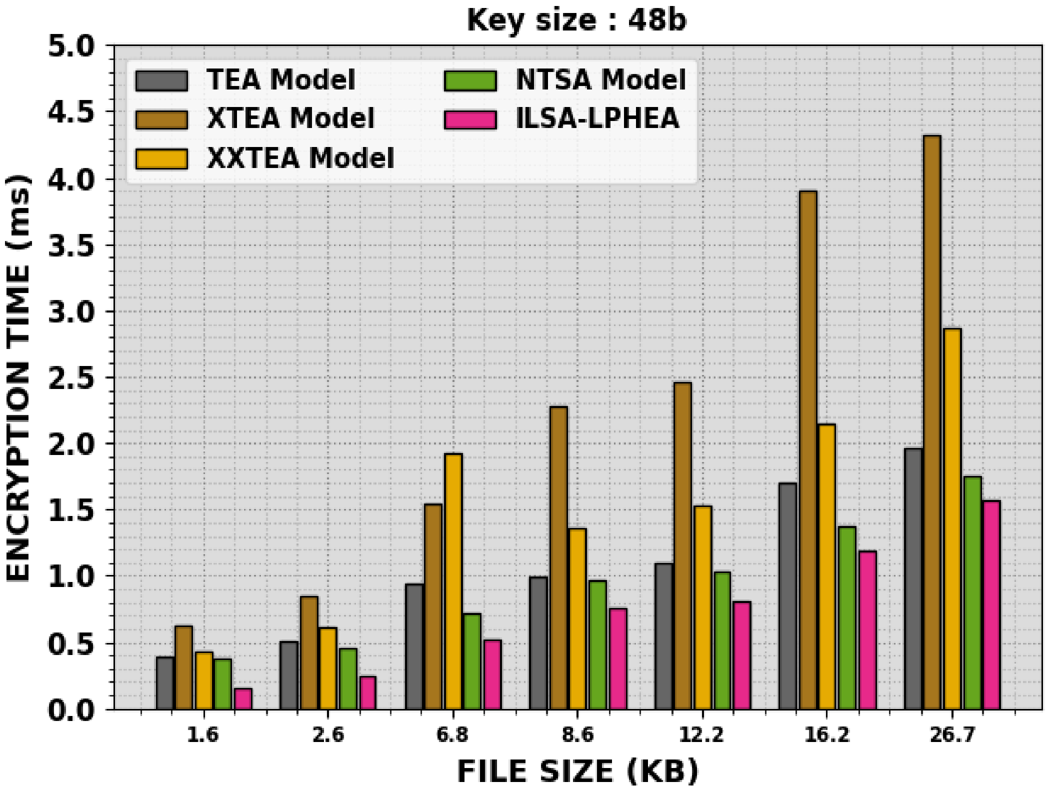

Figure 4. Outcome ofILSA-LPHEA algorithm underkey size of 48b

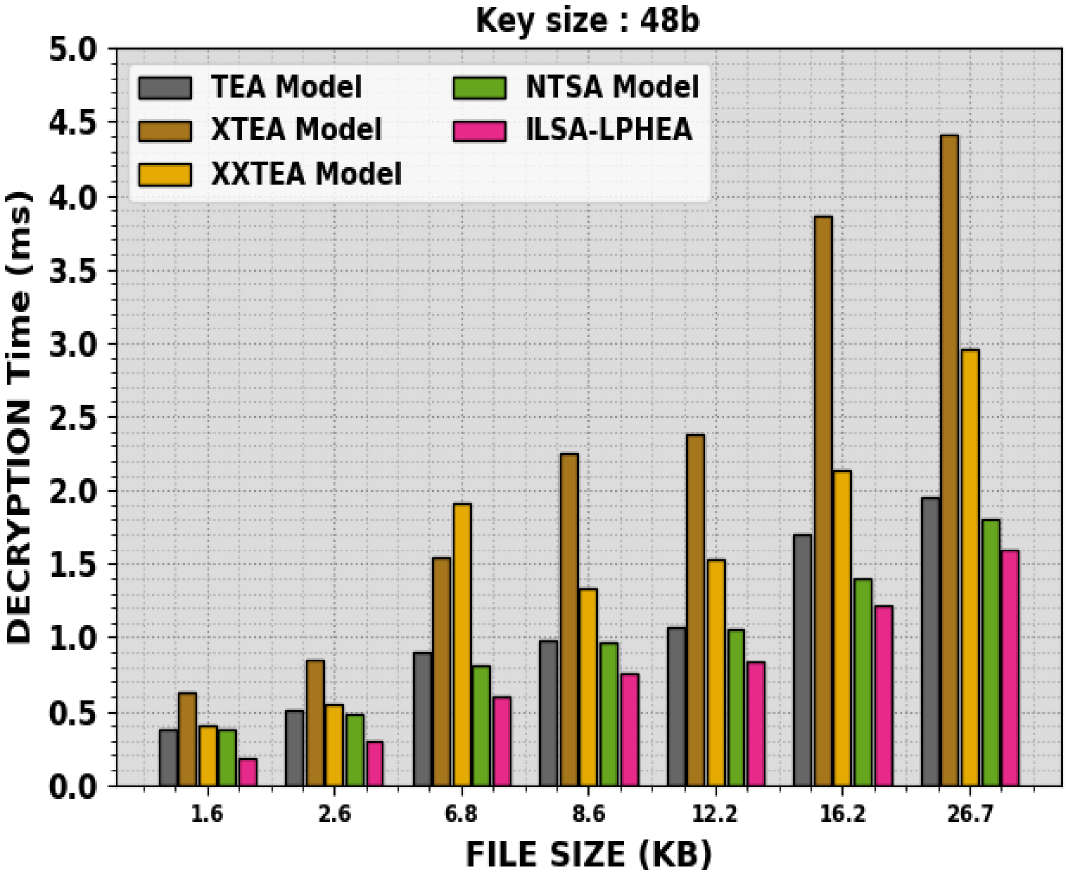

Figure 5. DT outcome ofILSA-LPHEA algorithm underkey size of 48b

In Table 2, the ET and DT analysis of the ILSA-LPHEA system with recent models are created on key size of 128b.In Figure 6, the comparison ET analysis of the ILSA-LPHEA method with key size of 128b is given. The figure exhibited that the XTEA and XXTEA systems get higher ET values. Simultaneously, the TEA and NTSA models obtain moderately reduced ET values. However, the ILSA-LPHEA system exhibits excellent performance with less ET of 0.123ms, 0.137ms, 0.475ms, 0.832ms, 0.901ms, 0.989ms, and 1.886ms, under file size of 1.6KB to 26.7KB, respectively.

In Figure 7, a comprehensive DT analysis of the ILSA-LPHEA method is compared with other encryption models with a key size of 128b. The obtained outcome demonstrated that the ILSA-LPHEA technique achieves the least DT values. With a file size of 1.6KB, the ILSA-LPHEA methodology offers reduced DT of 0.027ms while the TEA, XTEA, XXTEA, and NTSA models getraised DT values of 0.447ms, 0.250ms, 0.189ms, and 0.027ms correspondingly.

Table 2. ET and DT outcome ofILSA-LPHEA algorithm with other methods underkey size of 128b

Key size : 128b					
FILE SIZE (KB)	ENCRYPTION TIME (ms)				
	TEA Model	XTEA Model	XXTEA Model	NTSA Model	ILSA-LPHEA
1.6	0.249	0.473	0.282	0.238	0.123
2.6	0.380	0.737	0.431	0.273	0.137
6.8	0.747	1.631	0.792	0.600	0.475
8.6	0.997	1.719	1.221	0.947	0.832
12.2	1.326	2.855	1.586	1.069	0.901
16.2	1.171	3.312	1.913	1.149	0.989
26.7	2.259	5.257	2.276	2.032	1.886
DECRYPTION Time (ms)					
1.6	0.211	0.447	0.250	0.189	0.027
2.6	0.341	0.688	0.405	0.327	0.184
6.8	0.694	1.587	0.768	0.573	0.454
8.6	0.951	1.656	1.228	0.907	0.759
12.2	1.259	2.781	1.554	1.047	0.886
16.2	1.128	3.202	1.972	1.116	0.954
26.7	2.195	5.193	2.209	2.004	1.893

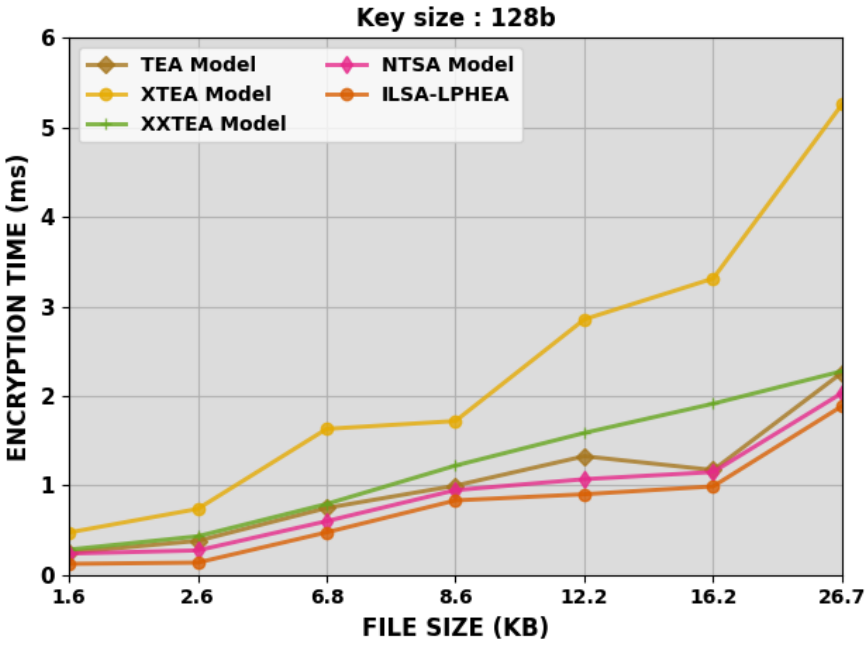

Figure 6.ET outcome ofILSA-LPHEA algorithm underkey size of 128b

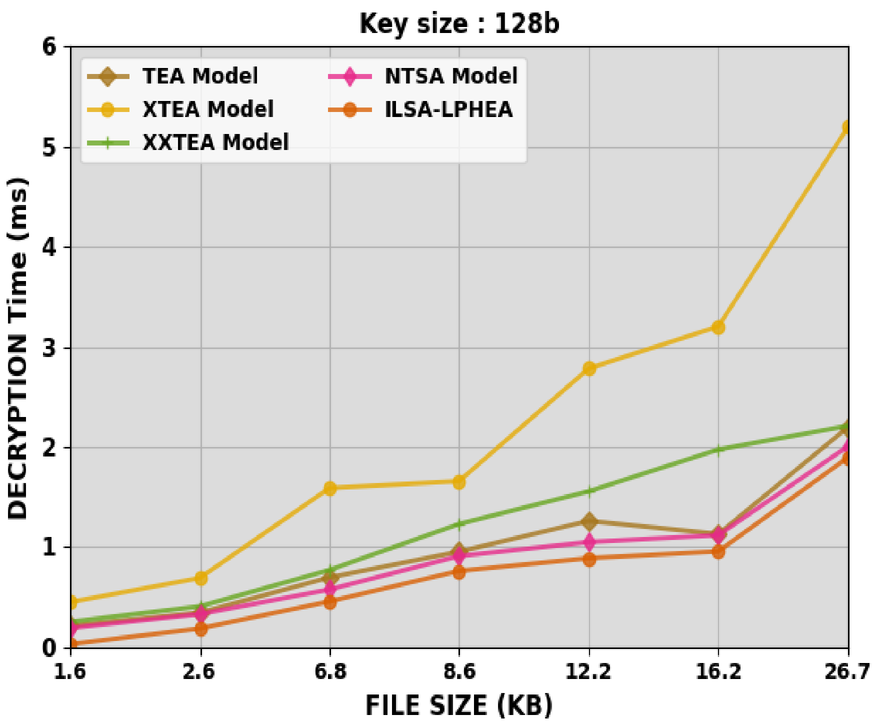

Figure 7. DT outcome ofILSA-LPHEA algorithm underkey size of 128b

In Figure 8 and Table 3, the ET and DT analysis of the ILSA-LPHEA system with recent models are generated with file size of 0.95kBb.

Table 3. ET and DT outcome ofILSA-LPHEA algorithm with other methods withfile size of 0.95kB

KEY SIZE (Bits)	File size : 0.95 kB				
	ENCRYPTION TIME (ms)				
	TEA Model	XTEA Model	XXTEA Model	NTSA Model	ILSA-LPHEA
32	0.242	0.414	0.264	0.194	0.038
48	0.239	0.414	0.288	0.210	0.042
64	0.244	0.378	0.284	0.201	0.034
96	0.266	0.394	0.304	0.212	0.037
128	0.276	0.377	0.269	0.218	0.052
160	0.244	0.420	0.281	0.216	0.064
192	0.274	0.420	0.287	0.242	0.073
240	0.237	0.390	0.288	0.227	0.069
	DECRYPTION Time (ms)				
32	0.255	0.393	0.258	0.215	0.052
48	0.257	0.391	0.290	0.233	0.055
64	0.271	0.339	0.275	0.215	0.036
96	0.259	0.377	0.279	0.222	0.056
128	0.245	0.398	0.323	0.207	0.046
160	0.246	0.383	0.280	0.223	0.057
192	0.268	0.406	0.276	0.244	0.091
240	0.267	0.398	0.296	0.257	0.100

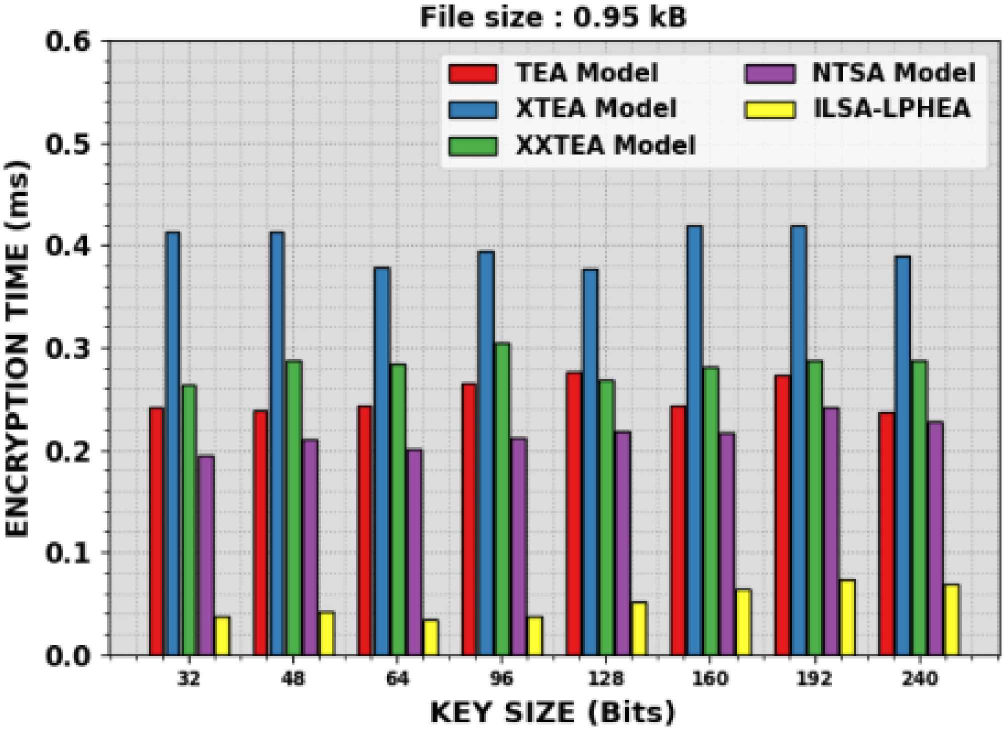

Figure 8. ET outcome ofI LSA-LPHEA algorithm under file size of 0.95kB

LPHEA systemshows greater performance with the lowest ET of 0.038ms, 0.042ms, 0.034ms, 0.037ms, 0.052ms, 0.064ms, 0.073ms, and 0.069ms, under key size of 32b to 240b, individually. In Figure 9, a detailed DT result of the ILSA-LPHEA methodcan be compared with other encryption methodologies with the file size of 0.95kB. The attained outcomeindicated that the ILSA-LPHEA technique achieveslesser DT values. With a key size of 32b, the ILSA-LPHEA modelgives decreased DT of 0.255ms while the TEA, XTEA, XXTEA, and NTSA models get improved DT values of 0.393ms, 0.258ms, 0.215ms, and 0.052ms respectively.

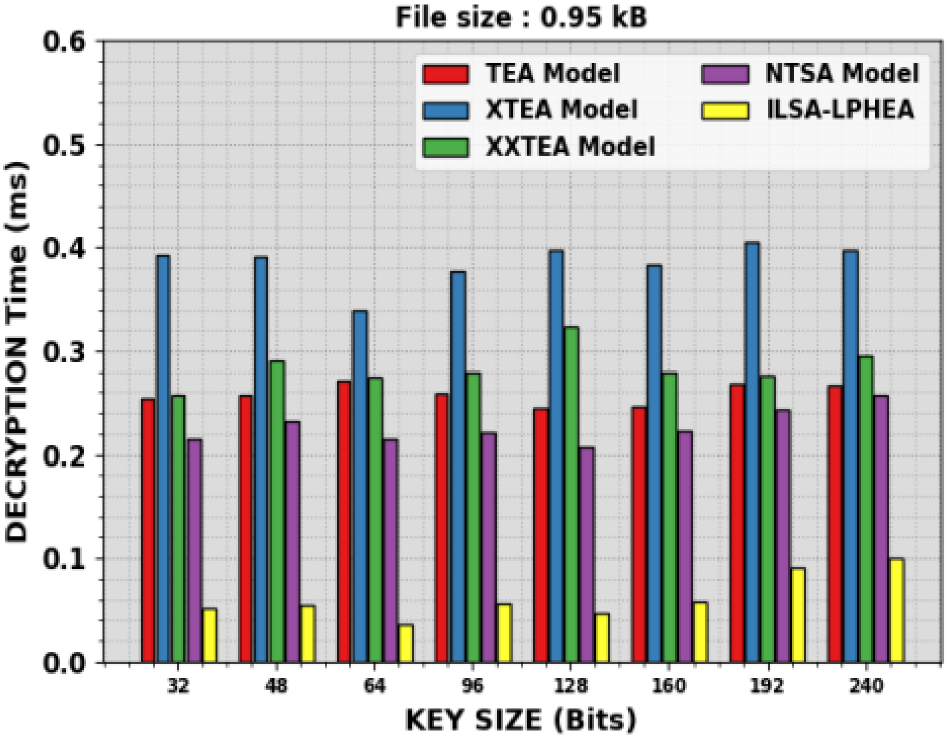

Figure 9. DT outcome ofILSA-LPHEA algorithm under file size of 0.95Kb

These results ensured the better performance of the ILSA-LPHEA technique over other models.

CONCLUSION

In this article, we have developed and designed a novel ILSA-LPHEA system for the security IoT environment via the LWC process. For securing the data from the IoT platform, the ILSA-LPHEA system makes use of the PHE approach. In addition, ILSA is used for optimal key generation, which enables to establishment of secure data transmission among the IoT devices and servers, the ILSA is used. With the application of ILSA, the optimal key generation process can be accomplished and it is significantly less resource-intensive. The hybridization of lightweight encryption with PHE strategy provides better security by enhancing privacy, confidentiality, and authentication, enabling end-to-end encryption. A detailed experimental result analysis highlighted the better solution of the ILSA-LPHEA system with other existing models. Therefore, the ILSA-LPHEA technique can be executed for end-to-end cryptographic solutions for the IoT environment.

Funding: The authors declare they have no funding applied.
Conflicts of Interest: The authors declare they have no conflicts of interest to report regarding the present study.

REFERENCES

1. Kumar A, Saha R, Alazab M, Kumar G. A lightweight signcryption method for perception layer in Internet-of-Things. J Inf Secur Appl. 2020;55:102662. http://dx.doi.org/10.1016/j.jisa.2020.102662.
2. Rao V, Prema KV. A review on lightweight cryptography for Internet-of-Things-based applications. J Ambient Intell Humaniz Comput. 2021;12:8835-57. https://doi.org/10.1007/s12652-020-02672-x.
3. Dejan S, Mladen T, Mladen V, Dejan S. An Application of Partial Homomorphic Encryption in Computer System with Limited Resources. Teh Vjesn. 2018;25(3):709-13. https://doi.org/10.17559/TV-20150928110055.
4. Medileh S, Laouid A, Euler R, Bounceur A, Hammoudeh M, AlShaikh M, et al. A flexible encryption technique for the internet of Things environment. Ad Hoc Netw. 2020;55:102240. https://doi.org/10.1016/j.jisa.2020.102662.
5. Vinoth Kumar K, Balaganesh D. An optimal lightweight cryptography with metaheuristic algorithm for privacy preserving data transmission mechanism and mechanical design in vehicular ad hoc network. Mater Today Proc. 2023;66(3):789-96. https://doi.org/10.1016/j.matpr.2022.04.304.
6. Mudra G, Cui H, Johnstone MN. Survey: An Overview of Lightweight RFID Authentication Protocols Suitable for the Maritime Internet of Things. Electronics (Basel). 2023;12(13):2990. https://doi.org/10.3390/electronics12132990.
7. Saba SJ, Al-Nuaimi BT, Suhail RA. A review of traditional, lightweight and ultra-lightweight cryptography techniques for IoT security environment. AIP Conf Proc. 2023;2475(1). https://doi.org/10.1063/5.0103349.
8. Gheisari M, Javadpour A, Gao J, Abbasi AA, Pham QV, Liu Y. PPDMIT: A lightweight architecture for privacy-preserving data aggregation in the Internet of Things. J Ambient Intell Humaniz Comput. 2023;14(5):5211-23. https://doi.org/10.21203/rs.3.rs-1771046/v1.
9. Vinoth Kumar K, Thiruppathi M. Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog Assisted Wireless Sensor Network. Acta Montan Slovaca. 2023;28(2). https://doi.org/10.46544/AMS.v28i2.18.
10. Rene CI, Katuk N, Osman B. A Survey of Cryptographic Algorithms for Lightweight Authentication Schemes in the Internet of Things Environment. 5th IC2IE. 2022:179-85. https://doi.org/10.1109/IC2IE56416.2022.9970015.
11. Rishabh, Sharma TP. Lightweight encryption algorithms, technologies, and architectures in Internet of Things: A survey. Innov Comput Sci Eng. Proc Int Conf 7th ICICSE. 2020;341-51. https://doi.org/10.1007/978-981-15-2043-3_39.
12. Khalifa M, Algarni F, Khan MA, Ullah A, Aloufi K. A lightweight cryptography (LWC) framework to secure memory heap in the Internet of Things. Alex Eng J. 2021;60(1):1489-97. https://doi.org/10.1016/j.aej.2020.11.003.
13. Thiruppathi M, Vinoth Kumar K. Seagull Optimization-based Feature Selection with Optimal Extreme Learning Machine for Intrusion Detection in Fog Assisted WSN. Teh Vjesn. 2023;30(5). https://doi.org/10.17559/TV-20211216115635.
14. Diro A, Reda H, Chilamkurti N, Mahmood A, Zaman N, Nam Y. Lightweight authenticated encryption scheme for the internet of Things based on publish-subscribe communication. IEEE Access. 2020;8:60539-51. https://doi.org/10.1109/ACCESS.2020.2983117.
15. Rajakani V, Vinoth Kumar K. Barnacles Mating Optimizer with Hopfield Neural Network Based Intrusion Detection in Internet of Things Environment. Teh Vjesn. 2023;30(6). https://doi.org/10.17559/TV-20211216115635.
16. Mahlake N, Mathonsi TE, Du Plessis D, Muchenje T. A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things. J Commun. 2023;18:47-57. http://dx.doi.org/10.12720/jcm.18.1.47-57.
17. Balakrishnan S, Vinoth Kumar K. Hybrid Sine-Cosine Black Widow Spider Optimization based Route Selection Protocol for Multihop Communication in IoT Assisted WSN. Teh Vjesn. 2023;30(4). https://doi.org/10.17559/TV-20211216115635.

18. Dwivedi A, Agarwal R, Shukla PK. Post-Quantum Lightweight Encryption Algorithm for Internet of Things Devices. In 2023 2nd ICEEICT. 2023;1-8. http://dx.doi.org/10.1109/ICEEICT56924.2023.10157055.
19. Anupama CSS, Alsini R, Supriya N, Lydia EL, Kadry S, Yeo SS, et al. Wind Driven Optimization-Based Medical Image Encryption for Blockchain-Enabled Internet of Things Environment. Comput Mater Contin. 2022;73(2):3219-33. https://doi.org/10.32604/cmc.2022.030267.
    Vinoth Kumar K, Balakrishnan S. Multi-objective Sand Piper Optimization Based Clustering with Multihop Routing Technique for IoT Assisted WSN. Braz Arch Biol Technol. 2023;66. https://doi.org/10.1590/1678-4324-2023220866.
20. Rajesh S, Paul V, Menon VG, Khosravi MR. A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. Symmetry (Basel). 2019;11(2):293. https://doi.org/10.3390/sym11020293.