International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Fortifying Patient Privacy: A Cloud-Based IoT Data Security Architecture in Healthcare

[*]Ajay Chandra MK
(Ajay Chandra Manukondakrupa)
[*]Department of Computer Science, Swami Ramanand Teerth Marathwada University, Vishnu Puri, Nanded, Maharashtra, 431606.
[*]Corresponding Author Mail id: ajaymanukonda88@gmail.com

Abstract

Concerns regarding patient privacy and security have been raised by the explosion in data generated by the growing use of IoT devices in healthcare settings. The absence of strong processes for authenticating individuals and devices in traditional healthcare systems leaves sensitive data open to potential breaches and illegal access. Since health care information is sensitive, maintaining confidentiality and integrity throughout the data's lifecycle is essential to safeguarding patient privacy and preserving public confidence in medical services. This research offers an extensive data security architecture designed specifically for cloud-based IoT healthcare systems in an effort to lessen these difficulties. The model uses robust encryption methods, including the Twofish algorithm, to protect sensitive data during transmission and storage. It also includes authentication procedures for users and Internet of Things devices. In addition, the model presents Energy-Included Lyrebird Fusion Optimization (EILFO) to identify the best key and key exchange process using is improved using the Elliptic Curve Cryptography (ECC)method. The suggested approach integrates these elements to provide effective data retrieval and storage in the cloud environment, while also strengthening data security by limiting access to patient information to those who are permitted. In addition to addressing current risks, this strategy lays the groundwork for enhancing confidence and trust in IoT-driven healthcare networks.

Keywords: *Patient privacy, IoT devices, cloud-based systems, Twofish algorithm, and Energy-Included Lyrebird Fusion Optimization (EILFO).*

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

1. Introduction

Cloud computing is one of the most important breakthroughs that has caught the attention of technologists worldwide. It is now essential for all cloud operations to identify the best solution instructions to boost cloud security [1].It is a massive data processing approach that combines computer technologies and networks to process and exchange data. A wide range of network resources can be made accessible to customers through the incorporation of cloud computing with software programs. Through computing technology, users of computers can access cloud resources at any location and time, enabling them to take advantage of the vast amount of data available and information resources on the network [2].Security issues with cloud computing will stop it from being widely adopted. The sharing of cloud computing resources makes it more difficult to prevent unwanted access or use and maintain security. The majority of data that is affected by this vulnerability is cloud-based data [3].

Typically, cloud computing research focuses heavily on task planning. The best completion time, the availability of resources, a quick reaction time, and high performance to employ helpful resources are requirements for many cloud computing positions. Amazon created many cloud computing platforms and popularized the idea of cloud computing. For example, EC2[4].The best method for ensuring high levels of data transport and storage security is cryptography [5].A cloud may be private or public. A private cloud is an enclosed data centre or network that offers an environment as a service to a restricted number of users with particular authorization privileges [6].Customers of cloud services can communicate with cloud service providers and upgrade their computing capacity automatically as needed. One of the benefits of cloud computing is its ability to lower times for customers and operating costs [7].

It is an essential technology that offers an effective structure for preserving, organizing, and handling the data produced by the Internet of Things (IoT) devices. Users may access cloud server resources from any location at any time via mobile devices [8].Intrusion detection systems (IDS) have become the most popular part of computer systems security processes for

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

safeguarding cloud environments from various attacks and threats [9]. Capacity, accessibility, and Flexibility are among the benefits of cloud computing as compared to conventional storage or internet-based computing approaches [10].News reports claim that 68 million user credentials were exposed due to a security breach at the Dropbox storage service provider [11].

By keeping information in a local database as opposed to a central data repository, blockchain technology improves security and shields against attacks on the cloud system [12].Loss of control over data may result from uploading information from Internet of Things devices to cloud servers, data integrity issues, and significant delays if the local backup is erased [13].Hypervisor and Virtual machines (VMs) are tools that cloud providers employ to keep customers separate. Virtual network isolation and VMs can now benefit from technologies that offer notable security benefits [14].Network managers need to be able to keep an eye on each subsystem's security status in real time within the security domain and implement strong security rules for other interconnected subsystems to stop thread propagation to ensure system security in cloud configurations [15]. The primary contributions of the paper are as follows,

- Sensitive patient data is protected during both the transmission and storage stages by integrating secured encryption techniques, such as the Twofish algorithm.
- Control access to healthcare data and stop unwanted breaches by implementing authentication processes for individuals and IoT devices.
- Introducing the Energy-Included Lyrebird Fusion Optimization (EILFO) technique to strengthen key exchange security and optimal key selection.

The remaining sections of the document are arranged as follows: The literature review is in section 2; section 3 describes the specific proposed technique; section 4 compares the results of the proposed methodology with the state-of-the-art techniques; and section 5 provides a detailed conclusion.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

2. Literature Review

In this section, the recent existing papers related to the data security in cloud environment are discussed.

Tahir *et al* (2021) [16] have developed a novel paradigm called Crypto GA, which uses a Genetic Algorithm (GA) to address data and privacy integrity concerns. To safeguard cloud confidentiality and integrity of data, a cryptographic method was combined with the keys generated by GA for decryption and encryption. In this study, validation and testing are conducted using ten distinct datasets. Examination of the test results showed that the suggested method shields user data integrity and privacy from outside interference.

Krishnaveni *et al* (2021) [17] have described an overview of an effective feature selection and ensemble classification-based Intrusion Detection System (IDS) for cloud environments. This technique accurately distinguishes between regular and malicious network traffic behavior. By employing ROC-AUC and other evaluation metrics on a range of classifiers, the implementation was evaluated. When this approach was compared to other current methods, the findings showed a significant performance improvement.

Cha*et al* (2021) [18] have implemented the Secret Sharing algorithm and blockchain to solve concerns about the security of personal data in external cloud services and to enhance security and data integrity through distributed system architecture. Cloud Service Provider employs the blockchain to securely store user data from a distributed user base in a distributed system that is more secure than prior centralized solutions. This method outperforms previous studies in terms of data storage efficiency and transaction speed.

Adee and Mouratidis (2022) [19] have presented steganography and cryptography-based data security concepts for cloud computing. The work of art was constructed using Design Thinking and the Python programming language. The outcome of this research was a four-step

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

data security model based on the algorithms of Rivest–Shamir–Adleman (RSA), identity-based encryption (IBE), Least Significant Bit steganography (LBS), and Advanced Encryption Standard (AES). This method shields data from hackers, resulting in increased cloud security and data redundancy.

Bouchaala*et al* (2022) [20] have unveiled a cloud computing authentication system that is both effective and safe, as well as a key agreement solution. Two-factor authentication, fuzzy verifier, Elliptic Curve Cryptography, and other techniques are presented in this work. The scyther tool's informal and formal validation demonstrated our solution's resilience against a range of threats. In comparison to comparable efforts, the performance evaluation demonstrated the robustness and efficiency of our system.

Ramachandra*et al* (2022) [21] have shown how to secure massive data in a cloud setting using the Triple Data Encryption Standard (TDES) technique. By enlarging the keys in the DES to enhance data privacy and prevent intrusions, this approach offered a comparatively easier solution. The outcomes of the study demonstrated how well this strategy worked to protect massive healthcare data in the Cloud environment. Moreover, it displayed shorter encryption and decryption times.

Rupa*et al* (2023) [22] have revealed a homomorphic encryption method for IoT devices and the cloud that was based on Matrix Transformations and transpositions of each character's binary-converted ASCII values. Symmetric cryptography uses the same secret key for both decryption and encryption. A cryptanalysis of this algorithm showed that it was more robust against different types of attacks than the preceding encryption techniques.

Shyla and Sujatha (2022) [23] have recommended a technique using multi-stage authentication (MSA) and an optimized blowfish algorithm (OBA) to retrieve data securely and efficiently in the cloud. The data security, data retrieval, and MSA components make up this system. The binary crow search method was utilized to determine the key value. This approach

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

was extremely safe since the user cannot access the file without authenticating. This approach was used to study performance in Java, and several metrics were used to evaluate the results.

Song*et al* (2021) [24] have recommended CSSM, a cloud-based secure storage mechanism. To prevent the leaking of cryptographic materials, it employed a hierarchical management structure and integrated secret sharing with user passwords. The experimental findings showed that this approach was not only appropriate for protecting data from leaks at the storage layer but also capable of efficiently storing large volumes of cloud data without requiring a significant amount of processing time.

2.1. Problem statement

The problem statement obtained from the discussed literature review papers are compared in table 1.

Table 1: Comparison of the existing papers

Author's name and citations	**Aim**	**Methods used**	**Benefits**	**Drawbacks**
Tahir *et al* (2021) [16]	To Protect data and privacy integrity in the cloud	Genetic Algorithm with the cryptographic method	Protects user data privacy	Limited information on scalability
Krishnaveni *et al* (2021) [17]	To Develop an effective IDS for cloud environments	Feature selection and ensemble classification	Accurately distinguishes regular from malicious network traffic	May require fine-tuning
Cha*et al* (2021) [18]	To Enhance security and data integrity	Secret Sharing algorithm and blockchain	Improved data storage efficiency	Potential complexity

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Adee and Mouratidis (2022) [19]	To Improve data security in cloud computing	Steganography, cryptography, Design Thinking,	Increased cloud security	Implementation may require advanced technical knowledge
Bouchaala*et al* (2022) [20]	To initiate a safe cloud computing authentication system	Two-factor authentication, fuzzy verifier, Elliptic Curve Cryptography	Resilience against a range of threats	Complexity in integrating multiple authentication techniques
Ramachandra*et al* (2022) [21]	To Secure massive data in the cloud	TDES	Prevention of intrusions	Key management challenges
Rupa*et al* (2023) [22]	To Develop a robust encryption method	Homomorphic encryption based on Matrix Transformations	Robust against different types of attacks	Potential computational overhead
Shyla and Sujatha (2022) [23]	To Retrieve data securely in the cloud	MSA, OBA	Efficient data retrieval	Implementation complexity
Song*et al* (2021) [24]	To develop Secure storage in the cloud	CSSM	Protection from data leaks	Potential overhead

2.2. Research Gaps

Further investigation into the use of hybrid cryptography for efficient data security in cloud computing is necessary due to a number of research gaps. Initially, it is important to investigate the scalability of hybrid cryptography methods, particularly in large-scale cloud settings managing enormous volumes of data. To optimize these procedures for effective data management, it is

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

necessary to evaluate the performance impact that hybrid encryption and decryption operations have on cloud resources. Secondly, there exists a deficiency in comprehension of the robustness of hybrid cryptography against emerging cyber risks and attacks, including attacks centred on quantum computing or advanced persistent threats directed toward cloud infrastructures. The fundamental goal of research should be to create robust hybrid cryptography algorithms that can survive complex attacks and still operate at high speeds. Furthermore, there are no thorough frameworks or standards for smoothly incorporating hybrid cryptography into various cloud architectures, such as public, private, and hybrid clouds. Closing those gaps can help improve cloud computing environments' privacy and data security.

3. Proposed Methodology

Major components of the overall system include the Cloud, m IoT users ($U_1, U_2, \ldots U_n$), and n IoT devices ($n_1, n_2, \ldots n_N$). IoT devices either generate or hold big data that needs to be stored in the cloud. The cloud environment is where the data is kept. The key areas of emphasis for the suggested system model are data retrieval, encryption, and authentication. Users and Internet of Things devices are both subject to authentication. Access to the cloud environment for storing created big data is granted to approved IoT devices. The encryption method ensures data security before that happens. Quick indexing is suggested as a way to facilitate data retrieval. Only those who have been granted permission by the Cloud can access the data. An exchange policy for keys has been developed for decryption. Enhancing the security level is the main goal of the suggested system. The block diagram of the proposed data security model in cloud computing is shown in Figure 1.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

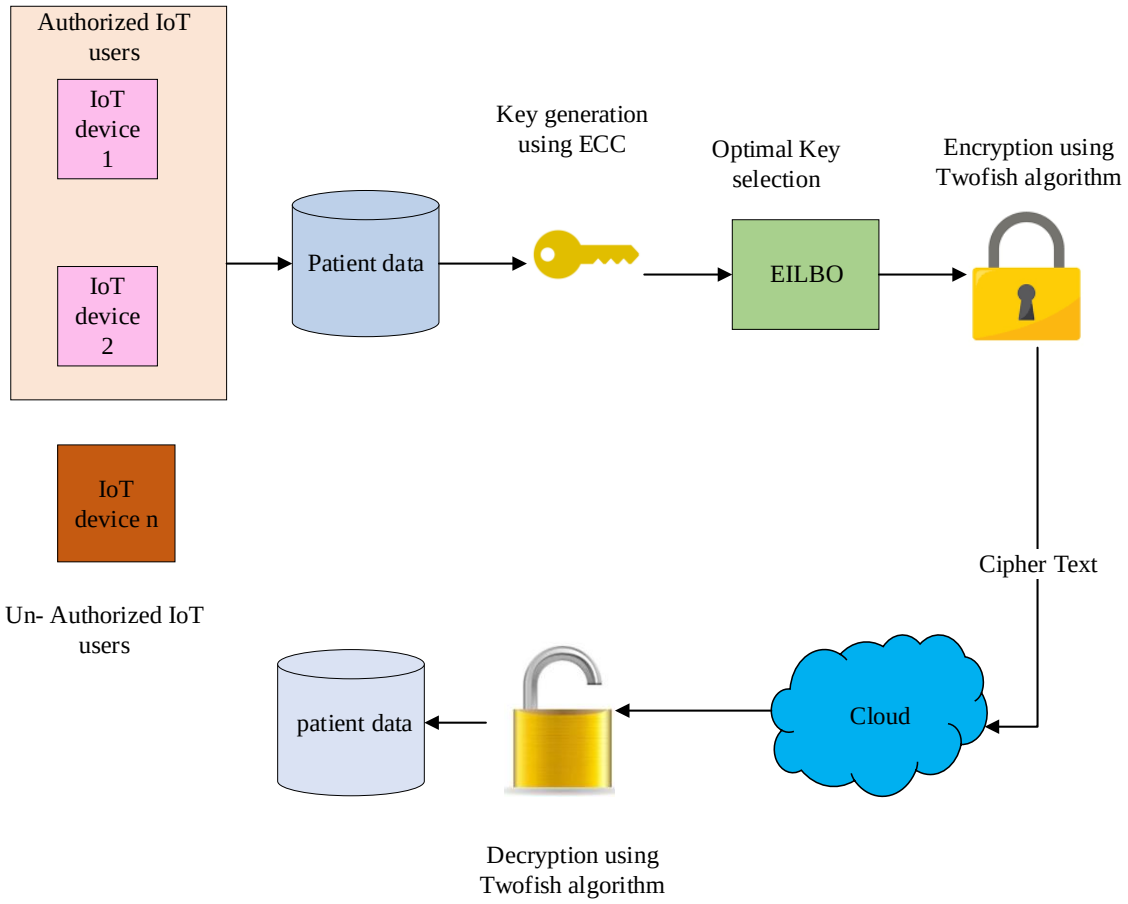

Figure 1: Work flow of the proposed data security model in a cloud environment

3.1. Data Collection using Authenticated IoT device

The patient has a sensor device fitted to their body as the first step in the recommended intervention. The Internet of Things device will use a sensor to identify the patient's physical characteristics and forward that information to an application for classification of illnesses. This section contains the tools, medical IoT sensors, and network equipment needed to identify and collect biological data from patients. The information gathered includes biological data as well as the patient's vital signs, which include blood pressure, heart rate, blood cholesterol, and others, as detected by sensors attached to the patient's clothing or body and perceived through the body area network. Both the

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

user and the device need to authenticate each time they need to access the cloud. The Device or User must provide their credentials to the Cloud in order to accomplish this task.

3.2.Upload patient's health records (PHR)

In this step, the patient's whole medical history, both current and prior, is uploaded to the twofish encryption. The PHR offers a wide range of data sizes. Because of this, the PHR is compressed and stored on the cloud server after being encrypted using the twofish technique. Prior to encryption, the ECC algorithm is used for both key generation and exchange procedures. It might produce additional keys; the EILFO method is used to choose the most ideal key from among them.

3.3. Key generation and Exchange using ECC

Create a robust data encryption plan for the Key Exchange in this research using the ECC technique. The main goal is to securely exchange tenant data while limiting access by unauthorized parties. The authentication method used in this study is ECC-based to ensure security. This method will result in a unique key value being provided by each user for both encryption and decryption. It will therefore stop unwanted users from getting access to other residents' sensitive information. Data is initially requested from the cloud by receiver end users, and access authentication is then used by the authentication server to limit access to the data. Verifying and granting authorized users' permission to modify data is the aim of the authentication process. ECC is an essential component of the recommended identity and data authentication process.

a. **Key Generation**:
   - Select an elliptic curve E that is defined over a large prime number (Fp).
   - Select a big prime number n such that nG is not the point at infinity and a base point G on the curve.
   - Select a private key d so that $1 \leq d < n$.
   - Determine the associated public key, $Q = dG$.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

b. Key Exchange:

- For encryption, the sender creates a random symmetric key K.
- The ephemeral key pair (r, R), where r is an integer selected at random and $R = rG$, is computed by the sender.
- Receiver's public key is B, and the sender calculates the shared secret point $S = dB$.
- From S, the sender obtains a symmetric key, K'.
- The symmetric key K' is used by the sender to encrypt the symmetric key K.
- The encrypted symmetric key is sent by the sender to the recipient.

c. Decryption

The recipient uses his private key $K = Dec(C, K')$ to decrypt the ciphertext he received. The decryption function employing the symmetric key K' is represented by Dec.

3.4. Optimal Key selection using Energy-Included Lyrebird Fusion Optimization (EILFO)

Every lyrebird that takes part in the EILFO chooses the values for the decision parameters according to where it is at that moment in the problem-solving domain. Consequently, all lyrebirds can be expressed mathematically as vectors, where a vector denotes a choice variable. All EILFO members make up the algorithm's population, and Eq. (1) permits mathematical modelling of them. The initial positions of LOA members in the problem-solving space are determined at random by using Eq. (2).

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} x_{1,1} & \cdots & x_{1,d} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{i,d} & \cdots & x_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,d} & \cdots & x_{N,m} \end{bmatrix}_{N\times m} \quad (1)$$

$$x_{i,d} = lb_d + r.(ub_d - lb_d) \quad (2)$$

In this instance, r is a random variable in the interval [0, 1], N is the total number of lyrebirds, m is the number of decision parameters, and lb_d and ub_d are the decision variable's

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

lower and upper bounds, respectively. X is the LOA population matrix, $X_i$denotes the i^{th}EILFOmember (potential solution), and $x_{i,d}$ denotes the d^{th}dimension in the search space. Using Eq. (3), one may obtain the vector representation of the set of evaluated values for the issue's goal value.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \quad (3)$$

The vector F contains all of the objective function values, with the value for thei^{th}EILFO component represented by F_i. The optimal choice is shown by the highest objective function value, and the worst alternative is indicated by the lowest objective function value.

i) Mathematical Modelling of EILFO

An exponential component is introduced to improve the Lyrebird's location update phase. The population update procedure consists of two stages: (i) concealing, and (ii) escape, depending on the lyrebird's decision in this case. In the EILFO design, Eq. (4) mimics the lyrebird's decision-making process when it must choose between hiding or running from danger. Every EILFO member's position is only changed during each iteration to comply with the first or second phase.

$$The\ update\ process\ for\ X_i: \begin{cases} based\ on\ Phase\ 1, & r_p \le 0.5 \\ based\ on\ Phase\ 2, & else \end{cases} \quad (4)$$

In this case, r_p is a random number within the range [0, 1].

- **Phase 1: Exploration Phase (Escaping Strategy)**

The EILFO phase updates the locations of population members in the search space using a model inspired by lyrebird flying. EILFO may demonstrate its capacity to carry out a worldwide search and exploration after relocating the lyrebird to a secure location. This leads to important positional modifications and investigation of other locations inside the problem-solving domain. The EILFO defines a safe region as the relative position of a member of the population with

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

higher objective function values. Each LOA member's set of safe zones can be found using Eq. (5).

$$SA_i = \{X_k,\ F_k < F_i \ and\ k \in \{1,2,3,\dots,N\}\} \text{ Where } i = 1,2,\dots,N \quad (5)$$

The i^{th}EILFO component ($F_k < F_i$) is less than the k^{th} row of the X matrix, represented as X_k, which has a bigger objective function value (F_k). SA_irepresents the collection of safe areas for the i^{th} lyrebird. Eq. (6) is used to determine the new location of each EILFO member based on the lyrebird movement modelling completed in this step.Through the integration of energy concerns, the algorithm is able to modify its escape method in response to the prey's energy levels. Because of its versatility, the algorithm can react to changes in the prey's behaviour or the environment more skilfully. The connected member's prior position is then substituted with this new location if the objective function's value is improved, in accordance with Eq. (7).

$$x_{i,j}^{P1} = x_{i,j} + E.r_{i,j}.(SSA_{i,j} - I_{i,j}.x_{i,j}) \quad (6)$$

$$E = E_1.E_0 \quad (7)$$

$$E_1 = c_1.\left(1 - \frac{t}{T}\right) \quad (8)$$

$$X_i = \begin{cases} X_i^{P1},\ F_i^{P1} \le F_i \\ X_i,\ else \end{cases} \quad (9)$$

E is the evading energy of prey. The prey's beginning energy is represented by E_0, a random number in the range [–1, 1], T is the maximum number of repetitions, c_1 is the standard constant which is set to 1.5, and $E_1$is the prey's diminishing energy.The i^{th}lyrebird's safe area is represented by SSA_iin this instance; its j^{th}dimension is indicated by $SSA_{i,j}$; the updated location is calculated based on the suggested EILFO's escape strategy, which is indicated by X_i^{P1}; the objective function value is represented by F_i^{P1}; random values from the interval [0, 1] are represented by $r_{i,j}$ and $I_{i,j}$are numbers that have been randomly selected as 1 or 2.

- **Phase 2: Exploitation Phase (Hiding Strategy)**

In this phase of EILFO, population members' locations inside the search space are modified to correspond with the lyrebird's plan to evacuate to a nearby safe haven. With this

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

tactic, the lyrebird's location is progressively altered as it cautiously surveys its surroundings and moves slowly in quest of a suitable hiding spot. This illustrates how EILFO is used locally in search operations. Using Eq. (10), EILFO simulates the lyrebird's movement toward a nearby appropriate hiding place in order to calculate each member's new position. If Eq. (11) is true, the objective function value carried by the associated member is replaced with the new location if it increases.

$$x_{i,j}^{P2} = x_{i,j} + \left(1 - 2r_{i,j}\right).\frac{ub_j - lb_j}{t} \tag{10}$$

$$X_i = \begin{cases} X_i^{P2}, & F_i^{P2} \leq F_i \\ X_i, & else \end{cases} \tag{11}$$

In this case, the iteration counter is t, random integers $r_{i,j}$ from the range [0, 1], the j^{th}dimension is represented by $x_{i,j}^{P2}$, the objective function's value is represented by F_i^{P2}, and the new location for the i^{th}lyrebird is chosen using the suggested EILFO's hiding technique. The patient's information is encrypted and sent via the Ethereum blockchain after choosing the key. The pseudocode for the HILBO algorithm is shown in Algorithm 1.

Algorithm 1: Pseudocode for HILBO algorithm

Initialize population X randomly within decision variable bounds
Evaluate fitness of each member in X using objective function F
Set iteration counter $t = 0$
Set maximum number of iterations T
Set constants: c_1, E_1
Set initial prey energy E_0
Repeat until convergence or maximum iterations reached:
  Increment iteration counter: $t = t + 1$
  Update population positions:
    For each lyrebird i in population:
      Generate random number r_p in range [0, 1]
      If $r_p \leq 0.5$: # Exploration Phase (Escaping Strategy)

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Determine safe area SA_i for lyrebird i using Eq. (5)

For each dimension j:

Calculate new position $x_{i,j}^{P1}$ using Eq. (6)

Evaluate fitness of new position F_i^{P1}

If $F_i^{P1} \leq F_i$:

Replace X_i with X_i^{P1}

Else: # Exploitation Phase (Hiding Strategy)

For each dimension j:

Generate random number $r_{i,j}$ in range [0, 1]

Calculate new position $x_{i,j}^{P2}$ using Eq. (10)

Evaluate fitness of new position F_i^{P2}

If $F_i^{P2} \leq F_i$:

Replace X_i with X_i^{P2}

Update prey energy E based on iterations and constants

Store best solution found so far

End Repeat

Return best solution found

3.5. Data Encryption using Twofish Algorithm

After completing the authentication process, the Internet of Things device can now encrypt the data. The suggested encryption algorithm takes the data's sensitivity level into account and is comparatively quick. Both parties can use the symmetric key with TwoFish to encrypt and decrypt the actual data after it has been safely transferred. Because of its speed and security, TwoFish is a good fit for this application. One of the encryption algorithms used for symmetric key block ciphers is called Twofish. Bruce Schneier is the designer, and it was selected as one of the Advanced Encryption Standard competition's five finalists. Twofish is an algorithm with a configurable key size and a block size of 128 bits. Twofish employ the Feistel network

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

architecture, which comprises XORing the remaining half of the text block at the conclusion of each cycle after passing half of it through a *F* function. Figure 2 depicts a typical Feistel network structure. One of Twofish'sadvantages is that its implementation is freely accessible to the general public and unrestricted by copyright, allowing anyone to utilize it.

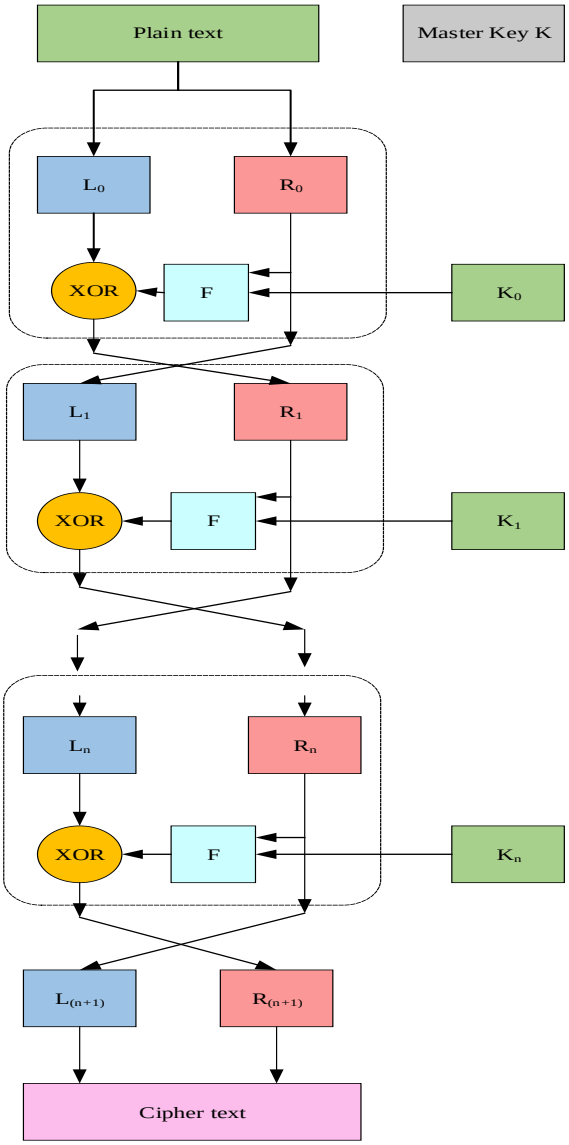

Figure 2: Layered architecture of the Feistel network

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

The F function takes two 32-bit words as input in each Twofish round. each word's four constituent bytes. We transmit the four bytes to four different key-dependent S-boxes. The S-boxes have 8-bit input and output, hence the four output bytes are aggregated into a 32-bit word using an MDS matrix. After merging the two 32-bit words using a Pseudo-Hadamard Transform (PHT), the right half of the divided text is appended to two round subkeys and XORed with them. Two 1-bit rotations are also taking place: one before the XOR and one after. Additionally, Twofish employs what are known as the "pre-whitening" and "post-whitening" strategies, in which extra subkeys are XORed into the text block prior to and following the final round.

3.6. Storage in cloud server

Following authentication, the encrypted data is prioritized and assigned to a particular cloud server. Priorities can be set according to a number of criteria, including the sensitivity of the data, the need for quick processing, or other business needs. Data must be sent to the correct processing unit or storage space inside the cloud architecture in order for it to be assigned to a particular cloud server. To increase the effectiveness of this allocation process, consideration might be given to how the workload is distributed throughout the cloud environment and the resources available on each server.

3.7. Data decryption using Twofish Algorithm

In this case, master keys are needed to decode the stored data. The user can decode the data if the secret and encrypted keys match; if not, the original data cannot be retrieved. Eventually, authorized individuals are given access so they can safely view their data. After the data has been decrypted, it is transmitted to the recipient end.

4. Result and Discussion

The data analysis by using Mat Lab into the various aspects of encryption, decryption, security. Key generation and upload time /download time for the different technique used in the data management. The techniques are Proposed TECC, Two fish, ECC, AES and HE.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

a. Encryption

Data is encrypted and made into a secret code that can only be decrypted with a special digital key in order to prevent it from being lost, altered, or compromised. The table 2 shows the encryption value of different dataset.

Table 2: Encryption values

Technique	**Encryption**
Proposed TECC	2.637
Two fish	4.559
ECC	5.048
AES	5.351
HE	4.59

Table 2 shows encryption methods and their respective millisecond (ms) execution times are displayed in the table. Data security requires encryption, which is essential, particularly in delicate fields like healthcare. The methods listed TECC (perhaps a new encryption approach), Two Fish, ECC, AES (Advanced Encryption Standard), and HE (Homomorphic Encryption) all have advantages and disadvantages that must be considered when evaluating security, effectiveness, and computational complexity.TECC stands out with the lowest execution time of 2.637 ms,

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

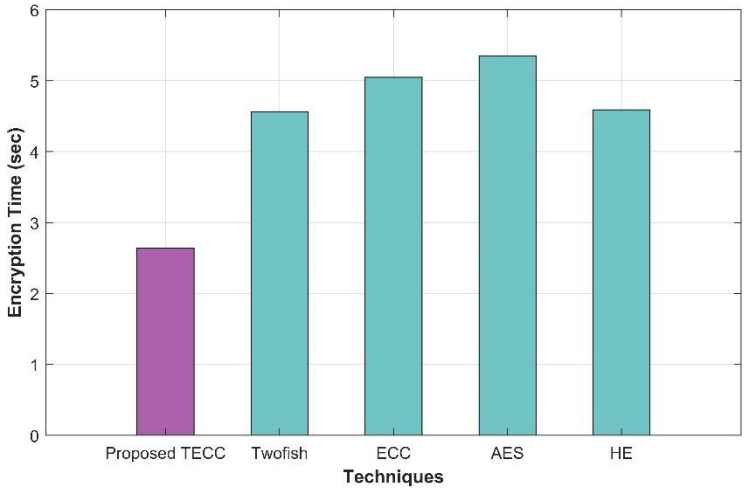

Figure 3: Encryption time analysis

Figure 3 show that the encryption value analysis. Encryption time analysis considered as seconds. The proposed TECC value stand for 2.637. it is a lower value compare to the other techniques. The other technique is silty higher then proposed TECC the value are Two fish =4.559, ECC=5.048, AES=5.351 and HE =4.59.

b. Decryption

Turning encrypted data back into its original form is called decryption. It is common practice to do the encryption process backwards. Only an authorized user is able to decrypt encrypted data since decryption requires a secret key or password.

Table 3: Decryption analysis

Technique	**Decryption**
Proposed TECC	2.764
Two fish	3.811
ECC	2.893
AES	3.319
HE	5.456

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

The table 3 provided lists the decryption timings (in milliseconds) for a number of encryption methods, including TwoFish, AES, ECC, HE (Homomorphic Encryption), and the suggested TECC method. An encryption's necessary opposite, decryption enables safe access to and interpretation of encrypted data by authorised parties.With a decryption time of 2.764 ms, the suggested TECC approach outperforms the other decryption techniques described, demonstrating effective decryption capabilities in addition to encryption.

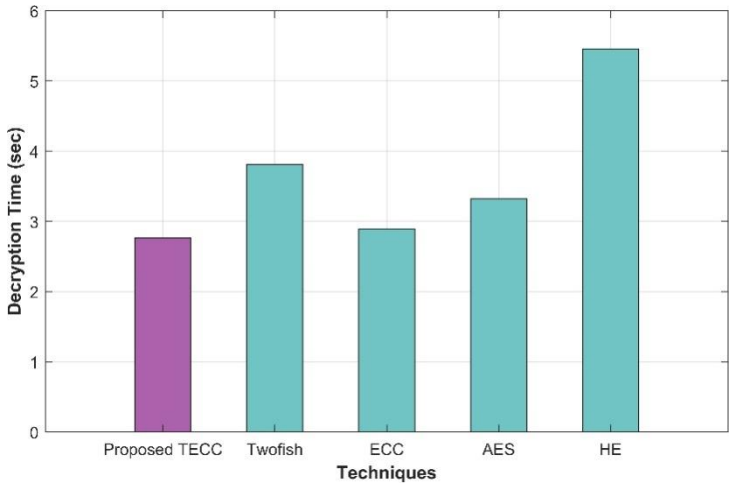

Figure 4: decryption value analysis

Figure 4 show that the encryption value analysis. decryption time analysis considered as seconds. The proposed TECC value stand for 2.764. it is a lower value compare to the other techniques. The other technique is silty higher then proposed TECC the value are Two fish =3.811,ECC=2.893, AES=3.319 and HE =5.456.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

c) Security

Table 4: Analysis of Security

Technique	Security
Proposed TECC	98.36
Two fish	95.46
ECC	95.49
AES	86.24
HE	83.07

Table 4 shows the security levels corresponding to different encryption methods are evaluated in the table and are shown as percentages. Encryption security is critical, guaranteeing that data is shielded from tampering and unwanted access. With a rating of 98.36%, the suggested TECC approach exhibits the maximum degree of security. This means that TECC has strong security procedures in place, which make it extremely resistant to breaches and attacks.

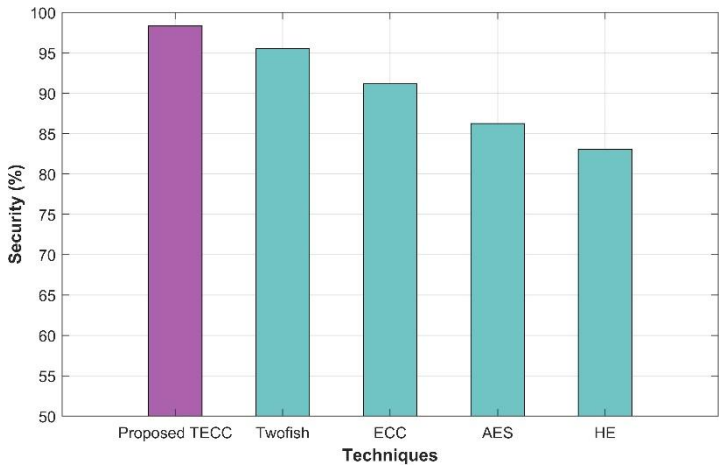

Figure 5: security value analysis

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Figure 5 show that the security value analysis. Encryption time analysis considered as percentage. The proposed TECC value stand for 98.36%. it is a lower value compare to the other techniques. The other technique is silty lower then proposed TECC the value are Two fish =95.46, ECC=95.49%, AES=86.24% and HE =83.07%.

d) Key generation

Table 5: Key generation table

Technique	**key generation**
Proposed EILFO	1.705
LBO	2.701
AB	2.144
GWO	3.584
GA [16]	2.975

Table 5 shows the essential generation times (in milliseconds) for a number of approaches, including Proposed EILFO, LBO, AB, GWO, and GA, are shown in the provided table. In cryptographic systems, key creation is an essential stage when secure keys are created for the encryption and decryption procedures. The fastest key generation time of 1.705 ms is demonstrated by the Proposed EILFO method, demonstrating its effectiveness in producing cryptographic keys. This implies that the EILFO approach might provide simplified key generation procedures, thus improving system performance in general.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

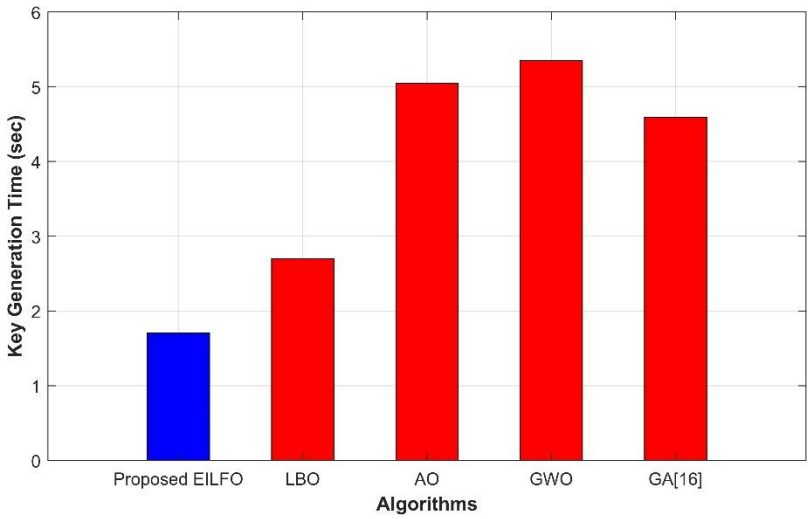

Figure 6: Key generation value analysis

Figure 6 show that the key generation value analysis. Key generation value analysis considered as seconds. The proposed TECC value stand for 1.705. it is a lower value compare to the other techniques. The other technique is silty higher then proposed TECC the value are Two fish =2.701, ECC=2.144, AES=2.144 and HE =2.975.

e) Uploaded time (ms)

Table 6 provides the uploaded times (in milliseconds) for a range of techniques and file sizes (10 KB, 20 KB, 30 KB, 40 KB, and 50 KB) are displayed in the table.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Table 6: uploaded time of different data size

Technique	Uploaded Time (ms)				
	10(kb)	**20(kb)**	**30(kb)**	**40(kb)**	**50(kb)**
Proposed EILFO	0.71	1.1	1.2	1.25	1.3
LBO	1.4	1.5	1.53	1.55	1.61
AB	1.2	1.3	1.32	1.33	1.36
GWO	1.6	1.65	1.68	1.69	1.7
GA [16]	1.845	1.75	1.74	1.73	1.73

The term "uploaded time" describes how long it takes to upload files to a platform or system. This information is vital for evaluating system performance, particularly in applications where data processing and transfer are involved. The Proposed EILFO method shows the fastest upload timings among all stated strategies, with a range of 0.71 ms for a 10kb file to 1.3 ms for a 50kb file. .

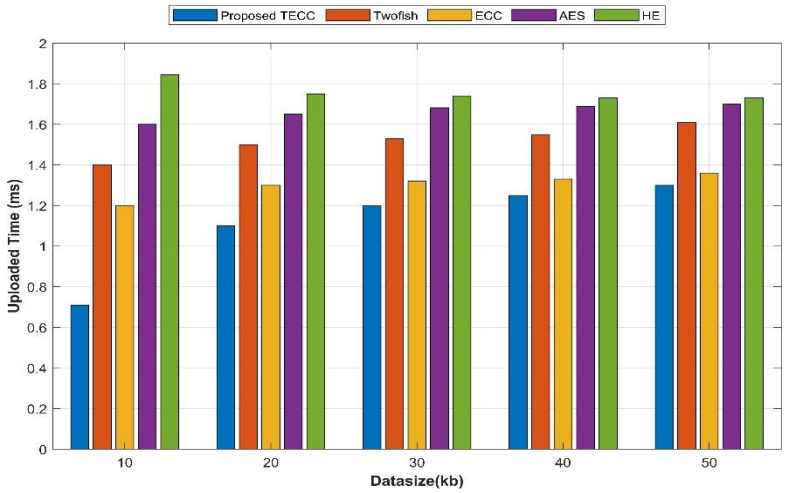

Figure 7: analysis of uploaded time for different data size

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Figure 7 shows the uploaded time for the different data size. The uploaded time in the different data size ranging from LBO=1.4 to1.61. AB =1.2to1.36, GWO = 1.6 to 1.7and GA [16] =1.845 to 1.73 (in GA is compared to other technique the value decrease in the level of 10kb to 50 kb.

f) Downloaded time (ms)

The table 7 shows the millisecond-based download times (in KB) for a range of approaches and file sizes (10 KB, 20 KB, 30 KB, 40 KB, and 50 KB). The term "downloaded time" describes how long it takes to get files from a platform or system.

Table 7: downloaded time of different data size

Technique	**Downloaded Time (ms)**				
	10(kb)	**20(kb)**	**30(kb)**	**40(kb)**	**50(kb)**
Proposed EILFO	0.33	0.35	0.38	0.39	0.42
LBO	0.71	0.73	0.76	0.78	0.81
AB	0.65	0.67	0.7	0.72	0.79
GWO	0.42	0.44	0.47	0.49	0.51
GA [16]	0.58	0.6	0.63	0.655	0.695

This is important information to know when assessing system performance, particularly for applications that need accessing and retrieving data. The Proposed EILFO approach shows the fastest download timings among all stated techniques, with download times ranging from 0.33 ms for a 10 kb file to 0.42 ms for a 50 kb file. This shows how well the EILFO method handles file downloads, which could lead to quicker data access and a better overall user experience.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

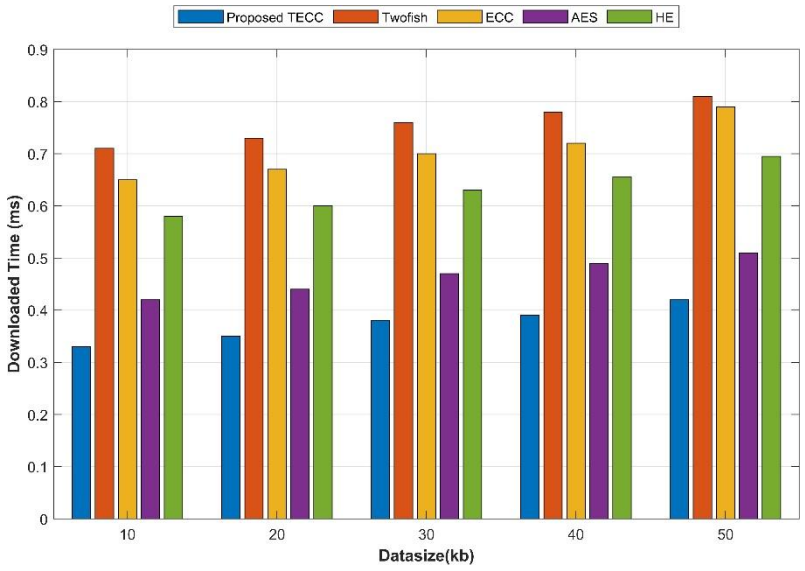

Figure 8: analysis of downloaded time for different data size

Figure 8 shows the downloaded time for the different data size. The downloaded time in the different data size ranging from LBO=0.71 to0.81 AB =0.65to0.79, GWO = 0.42 to 0.51and GA [16] =0.58 to0.61.

5. Conclusion

In conclusion, the growing use of IoT devices in the medical field has highlighted how critical it is to address issues with patient privacy and data security. Because traditional healthcare systems frequently lack strong authentication procedures, private information is vulnerable to intrusions and illegal access. This research suggests a thorough data security architecture designed especially for cloud-based IoT healthcare systems, acknowledging the necessity of preserving confidentiality and integrity throughout the data lifetime. To protect sensitive data both during transmission and storage, this architecture incorporates strong encryption techniques, such as the Twofish algorithm. Effective access control measures are put in place for users and IoT devices through authentication methods. In addition, the model incorporates EILFO to strengthen key selection and boost the process security of key exchange. Furthermore, the suggested method uses ECC to strengthen security in the key exchange procedure. By

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

combining these components, the model guarantees efficient data storage and retrieval in the cloud environment and fortifies data security by limiting access to those who are permitted.

Reference

[1]. Vinoth, S., Vemula, H.L., Haralayya, B., Mamgain, P., Hasan, M.F. and Naved, M., 2022. Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, pp.2172-2175.

[2]. Li, H., 2022. Computer security issues and legal system based on cloud computing. *Computational Intelligence and Neuroscience*, *2022*.

[3]. Thabit, F., Alhomdy, S., Al-Ahdal, A.H. and Jagtap, S., 2021. A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), pp.91-99.

[4]. Bal, P.K., Mohapatra, S.K., Das, T.K., Srinivasan, K. and Hu, Y.C., 2022. A joint resource allocation, and security with efficient task scheduling in cloud computing using hybrid machine learning techniques. *Sensors*, *22*(3), p.1242.

[5]. Chinnasamy, P., Padmavathi, S., Swathy, R. and Rakesh, S., 2021. Efficient data security using hybrid cryptography on cloud computing. In *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020* (pp. 537-547). Springer Singapore.

[6]. Raghavendra, S., Srividya, P., Mohseni, M., Bhaskar, S.C.V., Chaudhury, S., Sankaran, K.S. and Singh, B.K., 2022. Critical retrospection of security implication in cloud computing and its forensic applications. *Security and Communication Networks*, *2022*.

[7]. Ding, L., Wang, Z., Wang, X. and Wu, D., 2020. Security information transmission algorithms for IoT based on cloud computing. *Computer Communications*, *155*, pp.32-39.

[8]. Wu, T.Y., Meng, Q., Kumari, S. and Zhang, P., 2022. Rotating behind security: A lightweight authentication protocol based on IoT-enabled cloud computing environments. *Sensors*, *22*(10), p.3858.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

[9]. Al-Ghuwairi, A.R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A. and Algarni, A., 2023. Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. *Journal of Cloud Computing*, *12*(1), p.127.

[10]. Awan, I.A., Shiraz, M., Hashmi, M.U., Shaheen, Q., Akhtar, R. and Ditta, A., 2020. Secure framework enhancing AES algorithm in cloud computing. *Security and communication networks*, *2020*, pp.1-16.

[11]. Garg, N., Bawa, S. and Kumar, N., 2020. An efficient data integrity auditing protocol for cloud computing. *Future Generation Computer Systems*, *109*, pp.306-316.

[12]. Badri, S., Alghazzawi, D.M., Hasan, S.H., Alfayez, F., Hasan, S.H., Rahman, M. and Bhatia, S., 2023. An efficient and secure model using adaptive optimal deep learning for task scheduling in cloud computing. *Electronics*, *12*(6), p.1441.

[13]. Onyema, E.M., Dalal, S., Romero, C.A.T., Seth, B., Young, P. and Wajid, M.A., 2022. Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities. *Journal of Cloud Computing*, *11*(1), p.26.

[14]. Lanitha, B. and Karthik, S., 2020. Performance improvement of cloud security with parallel anarchies society optimization algorithm for virtual machine selection in cloud computing. *Soft Computing*, *24*(19), pp.15081-15092.

[15]. Xing, J. and Zhang, Z., 2022. Hierarchical network security measurement and optimal proactive defense in cloud computing environments. *Security and Communication Networks*, *2022*.

[16]. Tahir, M., Sardaraz, M., Mehmood, Z. and Muhammad, S., 2021. CryptoGA: a cryptosystem based on a genetic algorithm for cloud data security. *Cluster Computing*, *24*(2), pp.739-752.

[17]. Krishnaveni, S., Sivamohan, S., Sridhar, S.S. and Prabakaran, S., 2021. Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. *Cluster Computing*, *24*(3), pp.1761-1779.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 14 Issue 04, April- 2024
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

[18]. Cha, J., Singh, S.K., Kim, T.W. and Park, J.H., 2021. Blockchain-empowered cloud architecture based on secret sharing for smart city. *Journal of Information Security and Applications*, *57*, p.102686.

[19]. Adee, R. and Mouratidis, H., 2022. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), p.1109.

[20]. Bouchaala, M., Ghazel, C. and Saidane, L.A., 2022. Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart cards. *The Journal of Supercomputing*, *78*(1), pp.497-522.

[21]. Ramachandra, M.N., Srinivasa Rao, M., Lai, W.C., Parameshachari, B.D., Ananda Babu, J. and Hemalatha, K.L., 2022. Efficient and secure big data storage in a cloud environment by using triple data encryption standards. *Big Data and Cognitive Computing*, *6*(4), p.101.

[22]. Rupa, C., Greeshmanth and Shah, M.A., 2023. Novel secure data protection scheme using Martino homomorphic encryption. *Journal of Cloud Computing*, *12*(1), p.47.

[23]. Shyla, S.I. and Sujatha, S.S., 2022. Efficient secure data retrieval on the cloud using multi-stage authentication and optimized blowfish algorithm. *Journal of Ambient Intelligence and Humanized Computing*, *13*(1), pp.151-163.

[24]. Song, H., Li, J. and Li, H., 2021. A cloud-secure storage mechanism based on data dispersion and encryption. *IEEE Access*, *9*, pp.63745-63751.