Light Weight Cryptography based Medical Data and Image Encryption Scheme

M. Raja
Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India.
E-mail: kingraaja@gmail.com

Dr.S. Dhanasekaran
Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India.
E-mail: srividhans@gmail.com

Dr.V. Vasudevan
Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Tamil Nadu, India.
E-mail: vasudevan_klu@yahoo.co.on

Received March 10, 2021; Accepted July 06, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18I2/WEB18309

Abstract

Many medical companies use cloud technology to collect, distribute and transmit medical records. Given the need for medical information, confidentiality is a key issue. In this study, we propose an encrypted scheme based on encrypted data for an electronic healthcare environment. We use hybrid Attribute based encryption and Triple DES encryption technique (ABETDES) scheme, including identity-based cryptography (IBC), to ensure data privacy through communication channels և to improve the reliability of cloud computing. There are also limited indicators of light processing and storage resources. This solves a serious maintenance problem and ensures that a private key is created where it is not blind. The introduction of a security option, a comprehensive security analysis to protect ciphertext, shows that our program is effective against many known attacks and compared to existing methods.

Keywords

Light Weight Cryptography, Attribute based Encryption, Triple DES Encryption, Identity-based Cryptography.

Introduction

Every original lightweight cryptographer faces a compromise between security, cost and execution. Improving two of the three objectives of the project is generally simple: safety and costs, reliability, implementation or costs and implementation; However, it is difficult to advance the three objectives of the structure simultaneously (Eisenbarth et al., 2003). Light cryptography manages cryptographic calculations in relation to the strict requirements imposed on gadgets, for example the use of reasonably smart cards, sensor systems, electronic prostheses, which limit the use of dynamism, energy or material. Focusing on accessing shared information to customers or gadgets is fantastic or exceptional (Andreeva et al., 2014). Likewise, it is reasonable to assume full access to shared information if the cryptographic key is provided. However, nothing will be revealed. As a rule, this may not be enough (Ning et al., 2015). These days, an increasing amount of information is stored and obtained through distributed computing. Progress makes it a security issue. This implies that information can be effortlessly decoded and that the material and classification of information is lost by outsiders. We have introduced another calculation called "Cipher Attribute Based Encryption Algorithm" (Nalajala et al., 2019). Considering the presentation of the entry mandate, ABE offers us exceptional consistency and performance, thus naming the beneficiaries as a whole (Zhao et al., 2014). In an ABE line, a default private key can interpret ciphertext if it combines related properties and rules. ABE models can be divided into two types: ABE ciphertext policy (CP) and ABE and key-policy (KP) ABE (Lin et al., 2015), since the encrypted content is assigned to an access approach or has different characteristics.

In an Ciphertext-Policy ABE (CP-ABE) cryptographic conspiracy, each client has different characteristics and an uncomplicated key. A quality access strategy for the cryptographic part and a client can only decode if the client properties accept the strategy (Liu et al., 2016). This letter builds on the CP-ABE conspiracy to focus on the problem of stopping the presentation and the risk of greater governance and at the same time to understand better access control in portable interpersonal organizations. Multi-authority and multi-credit board levels (Luo., 2016) to ensure security and classification in the search for associates. First, the client needs to connect to the Internet and access a cloud server. The functionality of the organization is where information is sent and how it is encrypted. The secret text was created by trusted specialists, who provide this key for collecting information when customers of the information share their substances. In case they use the key and non-responsible information, the information client will restore it (Nalajala et al., 2019). Existing CP-ABE projects do not adequately address the progressive structure which is in essence in all circumstances. We propose a cryptographic framework that considers

different levels of connection between clients (Sethi et al., 2019). A subsequent error is in the development of the ciphertext, in which the access control network is not actually connected to the secret instances. This allows attackers to decode unauthorized encrypted content, considering the fact that their unique secret key segment, intended to prevent them from conspiring, can be left behind in the decryption process (Tan et al., 2016).

Legally use a CP-ABE infrastructure in a cloud application, which can lead to open problems. All mysterious customer keys must be delivered from a fully assigned key authority (KA). This is a security risk known as a key store problem. In case KA knows the mysterious key of a framework client, it can decrypt the entire client's encrypted information, which completely contradicts the client's desire (Wang et al., 2016). Reciprocal documents are generally layered. This means that a grouping of records is divided into a few subsets of important strings that are located at different access levels. In the event that data records in the corresponding multilevel structure can be encoded by an embedded access structure, the costs for storing the encrypted content and the costs for the encryption could be saved (Wang et al., 2016). In a KP-ABE framework, the choice for the entry-level approach is made more by the key operator than by cryptography, which limits the adequacy and usability of the framework in common sense applications (Xu et al., 2015). In this test, we use Attribute Based Encryption (ABE) for differential access control using IoT-encoded information. A client is assigned a mysterious key that reflects the input structure, with the aim that the client can decode the ciphertext if and only if the information properties coordinate its input structure (Phuong et al., 2018). Our design offers some improvements by combining a client's character with the personality of the Attribute Authority (AA) in which the client is located. This leads to unique customer identifiers of their kind on the planet and the issue of protection against agreements has also been resolved (Yang et al., 2018).

Literature Survey

The Internet of Things (IoT) offers special and unmatched integration of mixed and indistinguishable end frames. It is widely used in many applications, for example to organize vehicles, microcontrollers, brilliant food companies, series sales, compact devices and the mechanical Internet. These applications develop countless IoT devices that can be found, managed, evaluated and distributed. There may be a possible violation of IoT gadgets, regardless of whether servers or sensors are identified. A scrubber can affect the sensor and record basic data, or a scraper can capture servers and operate the sensors accidentally. With this in mind, there is an incredible requirement for a solid, but simple, shared test track. The approval is given at this point before the data exchange between the

sensors and the server. Due to the limited battery inclusion of IoT devices, the general understanding of the approval should also be low. Sachan et al. (2019) proposed an approval method using dynamic cryptography linked to the existing open key cryptography where the customer efficiently produces the key that needs to be matched against a higher value. The logically created key, which uses any limit, is used for encryption and decryption. In addition, an improvement in security is proposed by introducing a control element that is based on advanced encryption. The proposed diagram is evaluated under programming conditions, e.g. IPv6 on individual low-power remote systems (6LoWPAN), which are often used for IoT applications.

The Internet of Things (IoT) is a further development that can be used in the cloud system. In a cloud-based IoT organization, passionate gadgets collect various data and move it to a cloud server. In all cases, it is important to ensure classification and access control to ensure customer confidentiality, as the information may include classified information about people. Attribute-based encryption (ABE) is a decent tool for meeting these requirements. In both cases, most ABE installations do not offer encryption, decoding of successful executives or adaptable and powerful strategies for customer activity and key selection. By Muhammad Ali et al. (2020) to respond to these requests, we offer a Light weight ABE at different levels (LW-RHABE). In our reality, the customer effort is great and most of the accounting is done by a cloud server. In addition, our diagram provides customizable and versatile key naming and rejection tools using different level models. In fact, in our model, the key assignment and customer rejection of each feature can be monitored through different key approvals. We provide the definition of security to the LW-RHABE, introduce its security into the standard model, and await the severity of the decisional bilinear Diffie-Hellman (DBDH).

Light encryption is a fast-growing research field that meets the security requirements of devices with limited resources. This demand stems from the ubiquitous mainstream IT applications that rely on RFID tags, where cost and it requirements limit the unpredictability of the configuration and make it too expensive to consider standard cryptographic settings. Alipi et al. (2014) proposed to consider appropriate methods and planning measures for the safety of local residents on limited equipment.

Vision of the World of Distributed Computing Virtual IT Basics Different places offer different resources shared by customers. Information security is probably the biggest test when users share information with a distributed computer framework. Cloud Provider, Provider-Approved Clients, Other Cloud Clients, Unreliable Clients, or External Harm Factors can ignore information security. Encryption is one of the answers to securing and

classifying the information stored in the cloud. In any case, encryption techniques are expensive and expensive for cell phones. Bahrami et al. (2015) proposed another basic technique that enables portable clients to store information on at least one nebula using pseudo-random change based on vulnerabilities. To protect client protection, specific technology for portable client gadgets can be used to store information on cloud width without the use of distributed computer assets for encryption. We consider the situation of the JPEG image as a relevant test for the presentation and evaluation of the proposed system. Our verification results confirm the confidentiality of our customers' data, but show that the proposed upgrade enables a structured execution that is better than existing encryption methods such as AES and encryption in JPEG encoders. We see the underlying circumstances of an attack on a particular method that indicates the level of security.

Remote Medical Sensor Systems (MSN) is one of the most important variables in eHealth innovations, where biosensors can record diverse or inclusive information about key parameters in a patient's body. However, the security and security of the data collected is a serious problem because the exact resource limit, security, and accessibility of MSN gadgets are a test, and the remaining parts are unresolved. In this article, we offer a lightweight and secure framework for MSN. The framework uses a hash tag based keys update framework and a signature innovation guaranteed by intermediaries to achieve efficient and secure broadcasting and better information management. We are developing a framework to ensure the confidentiality and security of information. Our infrastructure requires only encryption / decryption and hashing capacity with symmetric keys, so it is suitable for sensor hubs with ity power. And Daojing Hai et al. (2013) in a system of limited resources combined with practical engines and CPs, the proposed framework explores the implications of exploration and its gradual manifestation. Based on the information we have, it is the primary framework for secure broadcasting and access control of information for MSN.

Mohasseb and Arsh (2013) proposed another security mechanism for image and sound, which relies on the direct features of the digital juggling encoder, and most of the rules of image and video encoding are used in the first stage: entropy encoding. This upgrades enables coding and encryption of synchronous entropy and reduces the amount of frame distortion and resources required by controlling the number of encoder probability maps handled. Additionally, the proposed method does not significantly increase encryption and does not increase the size of the compressed image. In this sense, unlike standard encryption techniques, when deciding on a specific strategy for decoded images, the decoder can display the decoded / decoded image pieces. Furthermore, this type of encryption is not widely associated with avoiding errors. Unlike most square counts, the default graph does

not add extra bits to the encoded bit stream. The specific method can be applied to any image and sound encoder that uses encoding to count numbers. In all cases, the implementation of this report complies with the JPEG2000 standard. We present the ratings and estimates of this encryption method.

In a decentralized and attribute-based encryption (ABE) framework, each acquisition can be converted into an authority by assigning private clients to multiple clients by creating an open key. Such an ABE project can remove the burden of strong correspondence and community-based processing in the ABE diagram layout phase with many specialists, making it more attractive. At the end of the IEEE exchange on similar distribution projects, Ge et al. (2013), In the ABE Framework for Protection proposed an attractive decentralized ABE framework, which allows consumers to obtain better security and protection in the standard model. After careful evaluation of the framework, we conclude that the framework cannot withstand global attacks and therefore does not meet the essential security implications of the ABE framework.

Proposed Methodology

The lightweight privacy preserving E-health system has been introduced to protect confidentiality. Our IBE system solves the main problem of engagement of the IBE system. In reality, it depends on hybrid encryption technology and the WOA. Start and manage the E-health KGC system. It is clear, but curious, and after the association phase, the patient can send personal well-being data to a distant clinical focus. New keys are created for each movement to move information safely. These keys are coded using our IBE diagram. Downloading a new file means that the user must initially enter a key request, a key for ABE, 3 keys for TDES and another key authentication key. When a key request is issued, ABE performs an encryption process, which then returns the value of the encrypted text as input to the TDES algorithm. It gets a secret 168-bit key, which is divided into three 56-bit keys. Encryption of the first secret key, encryption of the second secret key and encryption of the third secret key. A total of 4 keys are required for individual encryption, and the key generation process is carried out by a third party. Therefore, a WOA for generating the key is included at this point in order to optimize the key.

Intention Goals

Our main goal is to create a cheap and safe way to protect your e-health from the IoT. Information on compiling related properties.

- **Content - based privacy:** The loss of transmitted data must remain.
- **Integrity:** The information must not be changed during the exchange.

- **Mutual authentication:** communicate units can be carried out mutually.
- **Anonymity:** The authenticity of the sender must remain hidden, with the exception of the clinical potential.
- **Pseudonymity:** Instead of authentic characters, it is important to use the name pseudonyms.
- **Forward secrecy:** If you determine the key of the current meeting, we cannot access the keys last used.
- **Escrow-free:** The KGC cannot access information that has been moved.
- **Blind user private key generation:** To ensure a high level of data security, the customer must obtain a personal secondary key without determining its validity.

Light Weight Cryptography Technique Goals

This section explains the five main purposes of using Light Weight Cryptography. Each security system must offer different security features to ensure installation privacy. These features are primarily defined as the goal of the security structure. These goals can be recorded in five main support classes.

- **Authentication:** This means that the nature of the recipient and sender needs to be confirmed before data can be transferred through the system.
- **Secrecy or Confidentiality:** As such, countless people perceive a protected area. This means that only an approved person can encrypt the message or material: none.
- **Integrity:** Integrity means that the content of the transmitted data is downloaded from the last destination (sender and recipient). The main type of stock is checking packets on IPv4 maps.
- **Non-Repudiation:** This means that neither the sender nor the recipient can mistakenly deny the sending of a special message.
- **Service Reliability and Availability:** Since secure developers primarily attack secure structures, this can affect the opening of the customer organization.

Hybrid Attribute based Encryption with Triple DES Encryption Technique

We offer another ABE-based facility for safe and patient-oriented participation in PHR in IT situations that are used in multi-owner environments. To address the key administrative challenges, we adequately isolate the framework's customers in two types of spaces, particularly society in general and individual spaces. Most Attribute-based encryption (ABE) is based on technical data, in which a lawyer responsible for food or KGC can create the finished private keys of the customers with their master data. In this way, the problem of key transport is characteristic, so that KGC can decrypt any encrypted content that is sent

to the customers of the frame by generating its mysterious keys each time. The basic disadvantages of the current framework are that the information exchange is not exceptionally secure and that another client can no doubt access the information in the information store. In addition, the framework does not distribute information according to the client properties. In this perspective, the proposed hybrid hybrid encryption technique as ABE-Triple DES Triple DES Algorithm of the Triple Data Encryption Algorithm (TDEA or Triple DEA), which uses the data encryption standard (DES). Triple DES provides an overall strategy to increase the size of the DES key to protect it from such attacks without the intent of a truly new computing cryptography.

Let's talk about *S* with many attributes and *A* input structures. For reasons of consent, we will specify (I_{enc},I_{key}) encryption contributions and the age of the keys separately. We have a CP-ABE $I_{enc},I_{key}) = (A,S)$, representation in a KP-ABE $(I_{enc},I_{key}) =(A,S)$ cryptocurrency. The CP-ABE trajectory with redistribution advantages (corresponding to KP-ABE) consists of five calculations.

The ***Setup(λ,U)*** layout is used as information for calculation security parameters and the representation of the property universe. Provides open PK parameters and an AES MK button.

Encrypt (PK,M,I_{enc}) uses Open PK parameters, an M message, and an access structure (resp. attribute set) I_{enc} as encryption algorithm. This causes the CT ciphertext.

KeyGen$_{out}$(MK,I_{key}) The main key generation algorithm uses the MK key and a number of attributes (or input structures) I_{key} as information and creates an SK private key and a TK modification key. With this procedure, the ABE method returns only one key.

Transform(TK,CT) uses a modification key TK for I_{key} ciphertext transformation calculation of encrypted text, and an encrypted CT encoded under if I_{enc}. $S \in A$ and the cause of the error, anything ⊥ else, are mainly encrypted ciphertext CT'.

Decryptout(SK, CT' ***)*** uses a personal SK key for I_{key} decryption calculation and a partially decoded ciphertext CT' initially encoded in I_{enc}. If $S \in A$ is on, *M* returns the message it is an error symbol ⊥ otherwise.

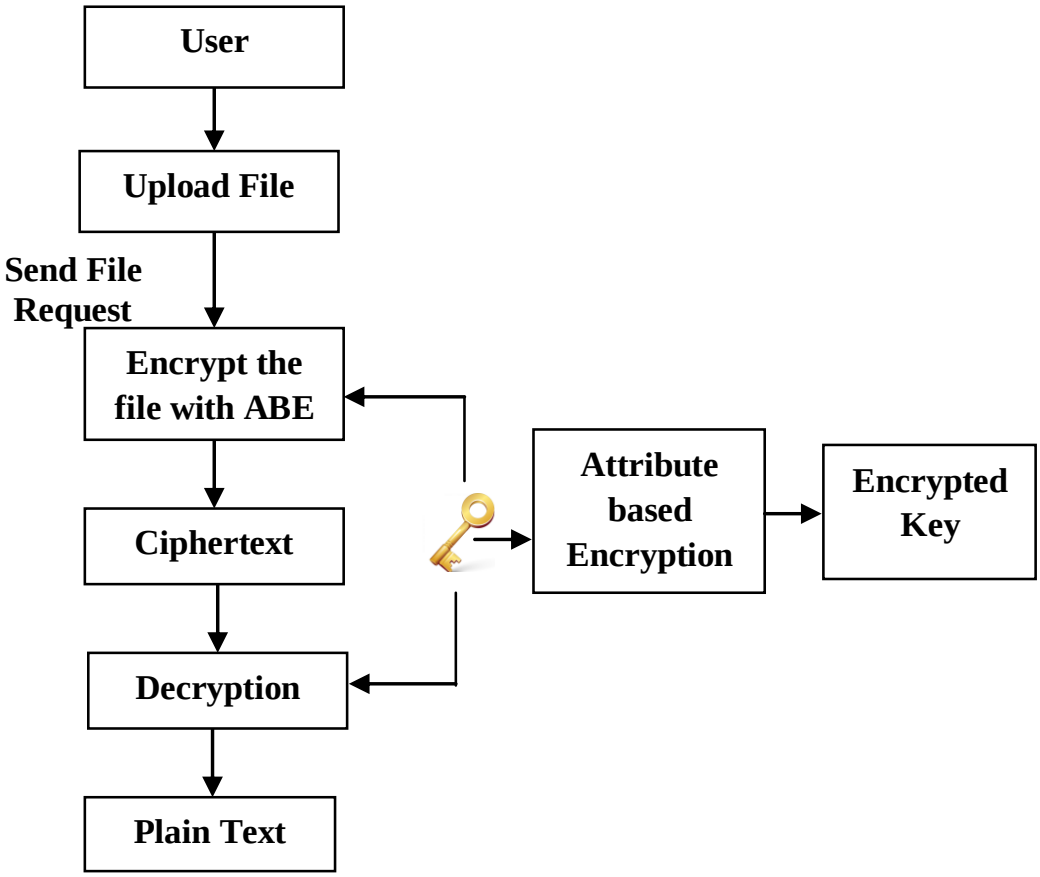

Figure 1 Process of Attribute based Encryption

During this time, the ciphertext was converted into a contribution to the triple DES procedure. 3DES Encryption Standard (Triple DES) DES has proposed an update. In this dimension, the coding method is similar to a single DES but used repeatedly to create the coding layer. Triple Data Encryption Standard (DES) is a type of electronic cryptography in which four-digit numerical calculations are used multiple times in each reference field. The main size has been extended to triple DES to provide additional security for the encryption feature. Each square contains 64-bit information. The three keys for each key are called 56-bit pack keys. There are three input options for information encryption:

- All keys being independent
- Key 1 and key 2 being independent keys
- All three keys being identical

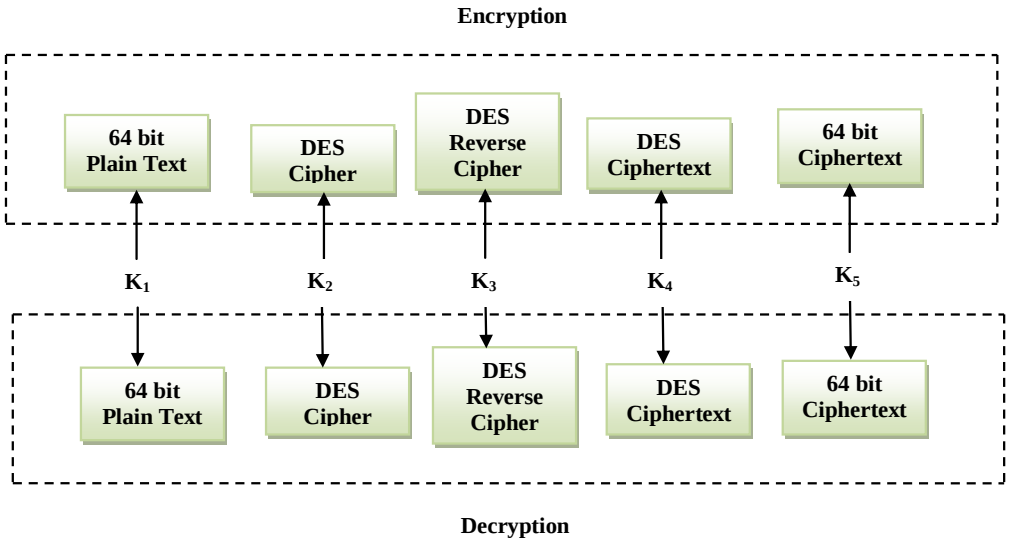

Figure 2 Process of Triple DES Technique

(i) Algorithm

Run the DES three times:

ECB mode

If K2 = K3, then it is DES
Backward Compatibility
DES is not the only one with K4
352 = 168 No, 112-bit security is available
The Triple DES algorithm uses three repetitions of the standard DES code. It obtains the 168-bit secret key, which is divided into three 56-bit keys.

- The first secret key to encryption
- Second encryption of the secret key
- Encrypt the third secret key

Encryption

$c = E3 (D2 (E1 (m)))$

Decryption

$m = D1 (E2 (D3(c)))$

Using a decryption in the subsequent coding phase provides an inverse similarity to the standard DES calculation. The keys to this situation are the first and second secret keys and the second and third secret keys.

$c = E3 (D1 (E1 (m))) = E3 (m)$
$c = E3 (D3 (E1 (m))) = E1 (m)$

The secret 112-bit key can be unlocked with the 3DES code. The first and third mysterious keys are not clear from this situation.

$c = E1 (D2 (E1 (m)))$

Triple DES is advantageous in that it has a more pronounced key length than the main coverage lengths associated with other encryption modes. The DES calculation was transplanted with the extended encryption standard, and the triple DES is currently decreasing. Although it comes from DES, this strategy uses a triple: contains three variable keywords and a keyboard. The keys must be distributed up to 64 bits. Triple DES is known for its similarity - adaptability - can be changed without inclusion.

Whale Optimization Algorithm

The sector is dominated by a digital model, including the harassment of hunting and bubble net, which leads to the development and search for hunting.

- **Encircling Prey**

Humpback whales can see and divide hunts. The position of the ideal structure in the field of observation or research is not known from previous positions. The WOA Improvement Calculation assumes that the best competitive transaction is currently targeted or close to matching. For this situation, cotton balls have been described as the best localization operator. Other hunting professionals will try to turn their situation into a better search engine at this point. This behavior can be introduced in related situations.

Humpback whales can move and move around the prey area. The position of the appropriate society in the public prosecutor's office or exam room is unknown from previous positions. The computation of the progress of the WOA recognizes that the best deal for the future is the target prey or approaching the ideal. In this case, humpback whales are considered an excellent investigative specialist. Other hunting companies are trying to pass on their status

to a specialist who is under investigation. This behavior can be described by the following conditions:

$$W = \left| f.\vec{x}^{*}(t) - \mathrm{f}\,\vec{x_i}(t) \right| \qquad (1)$$

$$\vec{x_i}(t+1) = \vec{x}^{*}(t) - \mathrm{B.W} \qquad (2)$$

Where *t* current is iteration, *A* and *C* are coefficients numbers. The module displays duplicate by component. Size of the hunting operator (population size) *X* is the state of the i^{th} whale with the × number of sizes. $\vec{X}\times$ is the location of the best setting Vector (optimal case scenario for the location operator) size 1 × is the set of estimates obtained up to this point || Its characteristic is a simple and simple value. It $\vec{X}\times$ is important to update for each accent when there is a higher order. *B* and *E* coefficients can be explained scientifically using the following terms:

$$B = 2b.r - b \qquad (3)$$

$$f = 2.r \qquad (4)$$

As a result, *b* is reduced to 2 to 0 during the cycle. This is common for the equation of (5), where t is the number of nodes and Max_{iter} most frequent iterations of the maxima. Where r is an arbitrary number in [0,1]. With bubble net upgrades, template shoots can attack hunters.

$$b = 2 - \mathrm{t} \times \frac{2}{\max_{iter}} \qquad (5)$$

B1. Bubble-Net Attacking Method (Exploitation Phase)

Two methods have been developed to scientifically demonstrate the bubble net performance of humpback whale:

Shrinking encircling mechanism: This strategy is attained by subtracting an incentive from the value of an in equation 12. A is an arbitrary range estimate, which *a* is decreases from 2 to 0 during accentuation. By the property of A in [-1, 1], one is able to visualize the new situation and the current ideal operator situation of a hunting expert near the operator's unique position.

Spiral-updating position: To spiral the helical development of humpback whales, meanwhile a helix-shaped state was established:

$$\vec{x_i}(t+1) = W.\mathrm{e}^{\mathrm{b}\int\cos(2\Pi\int)} + \vec{x^{*}}(t) \qquad (5)$$

Where $W = \left| x^{*}(t) - \left| x_i(t) - \right| \right|$ is the difference between i[th] whale and related people (the best arrangement so far). *b* is a coherent logarithmic winding and an arbitrary number in l [-1, 1], which is equal to the increase of the two elements of the layer.

During the leveling phase, humpback whales flow through the prey or rotate. 50% was chosen by removing the housing and winding, for example to update the location of the moving space. So the numerical model of this behavior can be given as follows:

$$\vec{x}_i(t+1) = \begin{cases} \vec{x}^{*}(t) - \text{B.W} & if p < 0.5 \\ W.f^{b\int}.\cos(2\prod\int) + \vec{X}^{*}(t) & if\ P \geq 0.5 \end{cases} \quad (6)$$

Where *p* is a number that is confirmed in [0.1]. Whatever the novelty of the bubble-net chain, the humpback whales code precedes it. The logical test model is as follows.

B2. Search for Prey (Exploration Phase)

A similar method can be used, which depends on the variable of parameter *A*, to search for the victim. Humpback whales are searched arbitrarily because they indicate a mutual condition. We use this to convince research experts to switch from reference whale *A*, which has more than *1* or less than *1* linear properties, to force search agents. Instead of the abuse phase, we update the status of a tracking expert in the request phase to indicate that the search operator selected is more unusual than the best hunting operator ever found. This system $|A| > 1$ increases demand and enables the study of WOA calculations worldwide. The digital model can be represented as:

$$W = f.\vec{X}_{rand} - \vec{X} \quad (7)$$

$$\text{X}_i(\vec{t}+1) = \vec{X}_{rand} - \text{B.W} \quad (8)$$

The *X* rand is a vector of any position that is multiplied by 1 factor and is controlled by the current population. The calculation of WOA begins with some random formations. Each phase of the search engine updates its scripts for any selected search engine or the best configuration ever made. The investigation and abuse parameter is reduced from 2 separately. $|B| > 1$ Select Legal successor operator if $|B| < 1$ update the position of the search engines. Depending on the P, WOA can go through a tortuous "development cycle". Finally, the WOA calculation ends at the end of the measurement. Specifies the 3DES (Triple DES). The encryption technology of this standard is similar to that of the individual DES, but has been used three times to extend the encryption level.

Result and Discussion

In the following areas, we have shown that in the event of an attack, our plans exceed the corresponding plans. To ensure greater stability, we consider ABETDES as planned by our IBE schemes. This section examines the results of several studies to promote the presentation of the analyzed calculations. Table I contains a comparison of proposed and Existing Study in Mim Attacks.

Table I Comparison of proposed and Existing Study in Mim Attacks

File Size kb	Proposed	ABE+TDES	TDES	ABE
25	13.6682	16.91969917	18.07472764	20.97064101
50	15.66854	18.83132308	20.27409055	22.60676702
75	17.3698	21.2935623	23.1077198	25.71408902
100	21.26862	24.36070569	25.4505528	27.7458634

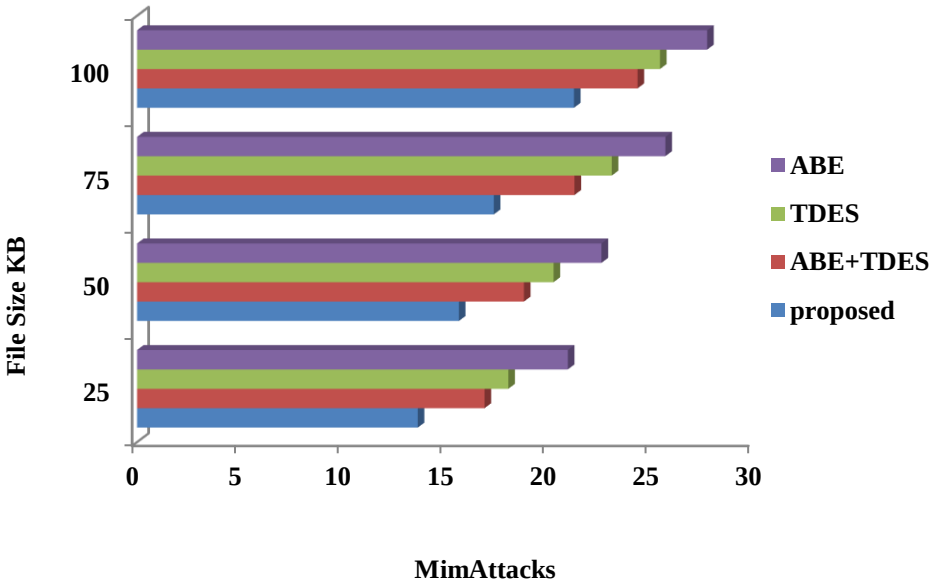

Fig. 3 Graphical representation of proposed and existing Mim attacks

The results are acceptable to provide an indication of the correlation results presented. Proposed, ABE+TDES, TDES and ABE have found that each of these methods provides, among others, the best execution of our proposed procedures.

Table II Comparison of proposed and existing Dos Attacks

File Size kb	Proposed	ABE+TDES	TDES	ABE
25	9.2554	13.59232222	15.01454673	16.11174087
50	10.268	14.52918743	16.42046433	17.57105407
75	12.97654	17.16639639	18.95884659	20.49968928
100	13.65945	17.79980392	18.9848535	20.46278608

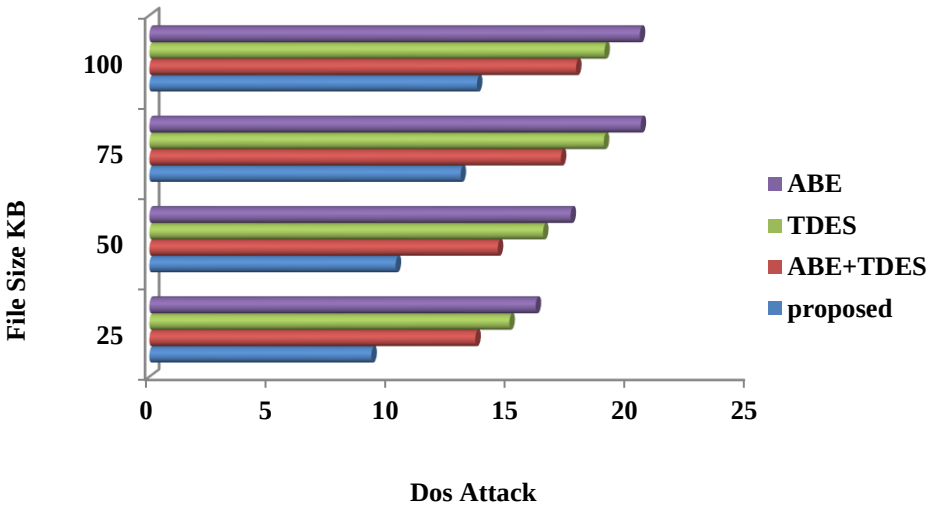

Figure 4 Graphical representation of proposed and existing Dos Attacks

In the current situation, many light cryptographic techniques are accessible, as shown in Table II. ABE + TDES are mainly used in the best security innovation. In the figure, the results show that the proposed procedure works differently for different calculations. The proposed procedure worked better than 3DES and DES.

Conclusion

Security is an important issue in E-health environments because of the impact of the data trade. In this paper, we proposed an efficient E-health framework based on another character-based cryptographic scheme called ABETDES. Our ABETDES confidence key not only corrects the problem of numbers, but also ensures the differential visibility of a private key. Presented without the security variation with the selected ciphertext. Our light weight cryptographic plans are used to ensure the secure transfer of keys. The effects of reproduction have shown that our cryptographic plans are as effective as existing plans. They are inexpensive and offer extreme protection. They are thus justified in the context of electronic well-being. Next, the proposed E-health program will be expanded to create rational provisions for information security.

References

Ali, M., Sadeghi, M.R., & Liu, X. (2020). Lightweight Revocable Hierarchical Attribute-based Encryption for Internet of Things. *IEEE Access*, *8*, 23951-23964.

Alippi, C., Bogdanov, A., & Regazzoni, F. (2014). Lightweight cryptography for constrained devices. *In International Symposium on Integrated Circuits (ISIC)*, 144-147.

Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mennink, B., Mouha, N., & Yasuda, K. (2014). APE: authenticated permutation-based encryption for lightweight cryptography.

In International Workshop on Fast Software Encryption, *Springer, Berlin, Heidelberg*, 168-186.

Bahrami, M., & Singhal, M. (2015). A light-weight permutation based method for data privacy in mobile cloud computing. *In 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 189-198.

Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., & Uhsadel, L. (2007). A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, *24*(6), 522-533.

El-Arsh, H.Y., & Mohasseb, Y.Z. (2013). A new light-weight jpeg2000 encryption technique based on arithmetic coding. *In MILCOM 2013-2013 IEEE Military Communications Conference*, 1844-1849.

Ge, A., Zhang, J., Zhang, R., Ma, C., & Zhang, Z. (2013). Security analysis of a privacy-preserving decentralized key-policy attribute-based encryption scheme. *IEEE Transactions on Parallel and Distributed Systems*, *24*(11), 2319-2321.

He, D., Chan, S., & Tang, S. (2013). A novel and lightweight system to secure wireless medical sensor networks. *IEEE journal of biomedical and health informatics*, *18*(1), 316-326.

Lin, S., Zhang, R., Ma, H., & Wang, M. (2015). Revisiting attribute-based encryption with verifiable outsourced decryption. *IEEE Transactions on Information Forensics and Security*, *10*(10), 2119-2130.

Liu, Z., & Wong, D.S. (2016). Practical attribute-based encryption: traitor tracing, revocation and large universe. *The Computer Journal*, *59*(7), 983-1004.

Luo, E., Liu, Q., & Wang, G. (2016). Hierarchical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks. *IEEE Communications Letters*, *20*(9), 1772-1775.

Ning, J., Dong, X., Cao, Z., Wei, L., & Lin, X. (2015). White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. *IEEE Transactions on Information Forensics and Security*, *10*(6), 1274-1288.

Nalajala, S., Akhil, K., Sai, V., Shekhar, D.C., & Tumuluru, P. (2019). Light Weight Secure Data Sharing Scheme for Mobile Cloud Computing. *In Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 613-617.

Phuong, T.V.X., Ning, R., Xin, C., & Wu, H. (2018). Puncturable attribute-based encryption for secure data delivery in internet of things. *In IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, 1511-1519.

Sachan, A., Kumar, N., & Adwiteeya, A. (2019). Light Weighted Mutual Authentication and Dynamic Key Encryption for IoT Devices Applications. *In International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 1, 1-6.

Sethi, K., Pradhan, A., Punith, R., & Bera, P. (2019). A scalable attribute based encryption for secure data storage and access in cloud. *In International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1-8.

Tan, S. (2016). Comment on "Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing. *In IEEE Access*, *4*, 1-4.

Wang, S., Liang, K., Liu, J.K., Chen, J., Yu, J., & Xie, W. (2016). Attribute-based data sharing scheme revisited in cloud computing. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1661-1673.

Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., & Xie, W. (2016). An efficient file hierarchy attribute-based encryption scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1265-1277.

Xu, J., Wen, Q., Li, W., & Jin, Z. (2015). Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing. *IEEE transactions on parallel and distributed systems*, *27*(1), 119-129.

Yang, Y., Chen, X., Chen, H., & Du, X. (2018). Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing. *IEEE Access*, *6*, 18009-18021.

Zhao, J., Gao, H., & Zhang, J. (2014). Attribute-based encryption for circuits on lattices. *Tsinghua Science and Technology*, *19*(5), 463-469.

Farzin, A., Yousefi, S., Amieheidari, S., & Noruzi, A. (2020). Effect of green marketing instruments and behavior processes of consumers on purchase and use of e-books. *Webology*, *17*(1), 202-215.