

Secured Health Data Transmission Using Lagrange Interpolation and Artificial Neural Network

S. Vidhya^{1,*} and V. Kalaivani²

¹Amrita College of Engineering and Technology, Nagercoil, 629901, India

²National Engineering College, Kovilpatti, 628503, India

*Corresponding Author: S. Vidhya. Email: vidhya.mahesh@ymail.com

Received: 25 January 2022; Accepted: 13 June 2022

Abstract: In recent decades, the cloud computing contributes a prominent role in health care sector as the patient health records are transferred and collected using cloud computing services. The doctors have switched to cloud computing as it provides multiple advantageous measures including wide storage space and easy availability without any limitations. This necessitates the medical field to be redesigned by cloud technology to preserve information about patient's critical diseases, electrocardiogram (ECG) reports, and payment details. The proposed work utilizes a hybrid cloud pattern to share Massachusetts Institute of Technology-Beth Israel Hospital (MIT-BIH) resources over the private and public cloud. The stored data are categorized as significant and non-significant by Artificial Neural Networks (ANN). The significant data undergoes encryption by Lagrange key management which automatically generates the key and stores it in the hidden layer. Upon receiving the request from a secondary user, the primary user verifies the authentication of the request and transmits the key via Gmail to the secondary user. Once the key matches the key in the hidden layer, the preserved information will be shared between the users. Due to the enhanced privacy preserving key generation, the proposed work prevents the tracking of keys by malicious users. The outcomes reveal that the introduced work provides improved success rate with reduced computational time.

Keywords: Cloud computing; homomorphic encryption; artificial neural network; lagrange method; cryptography

1 Introduction

The development of cloud computing has emerged as a significant factor due to its improved scalability and availability. Cloud computing exhibits unparalleled advantages and offers high efficiency and convenience [1,2]. Due to the advantages like increased security, reliability, high processing and storage ability, cloud computing is attracting more areas for the deployment of relevant applications and enables the storage of big data [3–5]. It facilitates the access of health records of patients/users from anywhere and at anytime. It permits the sharing, synchronization, storage and retrieval of data in cloud server [6]. Considering, health care applications, the privacy of the patient's data has to be preserved and hence



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

cloud storage is widely opted for this purpose. Numerous information related to heart beat, blood pressure etc. are constructed and stored in the cloud [7,8]. The data thus sensed has to be processed and analysed for providing enhanced care to patients in a prompt manner [9]. Moreover, the data has to be preloaded in the data centers of the cloud prior to its application requested by the user. Added to this, high cost of data transmission and extremely high response latency are to be considered in cloud related data transmission [10]. Cloud computing also faces numerous cyberattacks and these attacks rely on the security objectives and the threats faced. Although, basic security goals like integrity, confidentiality and availability are achieved by cloud service provider, the users require additional or prioritized security requirements [11]. Thus cloud computing has emerged as the primary source for the challenges and vulnerabilities related to security [12]. Numerous works have been carried out related to the secured data transfer in cloud computing. In [13], fuzzy based data transfer is carried out in cloud using fuzzy identities and the process of key generation is very simple with reduced computational complexity. The approach is lightweight and efficient but concentrates only on encryption and decryption of data. A multi-objective scheduling approach using fuzzy based resource allocation is proposed in [14] for the efficient transfer of data in cloud. The suggested method considers the account reliability constraints and reduces the cost yet does not check the significance of the data. In [15], a hybrid approach is introduced for the improved data security in cloud computing. An enhanced confidentiality and security of data is obtained in this work, but the key distribution has to be solved since the keys are not hidden. An approach for privacy in data sharing is proposed in [16] which uses Advanced Encryption Standard (AES) for improving the privacy and data integrity. However, in this approach, every block is encrypted in the similar manner. In [17], a privacy preserving data possession scheme is proposed based on identity using Rivest–Shamir–Adleman (RSA) algorithm assumption. Although, this approach efficiently verifies the integrity, it can be further enhanced in terms of security. A novel algorithm based on RSA is proposed in [18] to provide a secured data transmission in cloud. It reduces the storage complexity and enables key distribution between certified users, yet demands further improvement in security. The depiction of users searching the resources is significantly provided in Fig. 1 in an efficient manner.

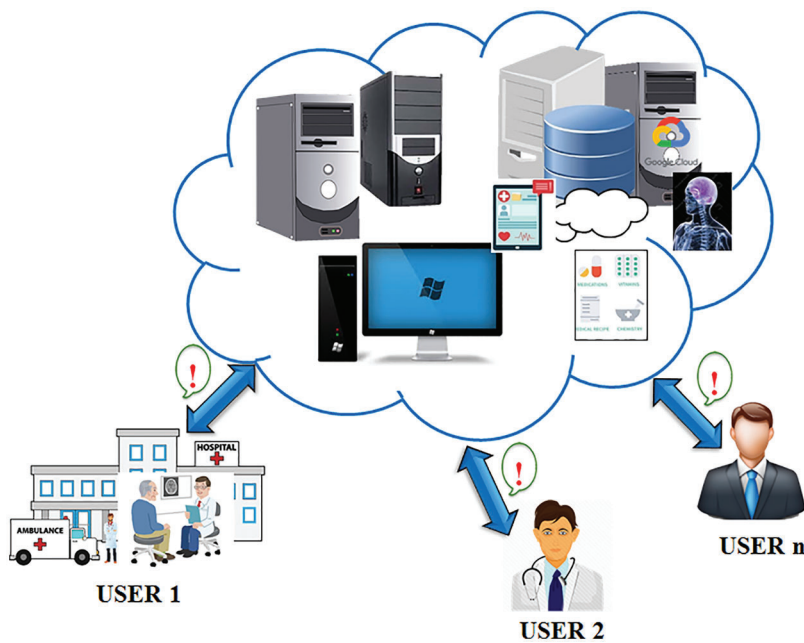


Figure 1: Users in search of finding resources

On the whole, the proposed work contributes an efficient secured approach for the transmission of health care data using cloud computing. The data stored in the cloud is categorized by ANN based on its significance as significant and non-significant data. Later, the significant data are encrypted by Lagrange interpolation and the encrypted data is stored in the hidden layers of ANN. When the secondary user provides a request for data, the primary user verifies the request and forwards the key to the mail of the secondary user. Henceforth, a privacy preserving and secured transmission of health care data is carried out in cloud.

2 Related Works

In [19], a novel hybrid cloud technique for sharing medical resources over a network is presented. In this paper, due to the lack of proper data sharing and poor interoperability features, a hybrid cloud method has been developed to induce effective data sharing. Even though the patients' data is exchanged between various providers, their privacy is not invaded. The issue arises with the consideration of a single language for data sharing, which may result in dispute while applying a unified data format.

In [20], an identity-based proxy oriented method is discussed for uploading the data in the cloud. In this paper, after examining various cryptography and algorithms, a new identity-based method has been proposed to undergo secured and efficient data sharing via cloud platform. The Efficient-Provable Data Possession (PDP) does not require any abundant encryption and it also allows the block renovation, deletion in an efficient manner. Since only the file owner can delete the uploaded file, an issue in the key remembrance may occur.

A lightweight searchable public-key encryption is proposed in [21] for cloud-assisted wireless sensor networks. In this paper, in order to increase the data confidentiality over the cloud storage which can help in the reduction of risk in cybersecurity, a public-key encryption technique has been proposed. The three structures used in this technique drastically reduce the complexity, the search tasks are examined for completeness and the most effective content search is possible in this technique. However, without a keyword search trapdoor, the eavesdropper may attack, as keywords are unknown and unpredictable to the cloud.

A key-aggregate cryptosystem is demonstrated in [22]. In this paper, to encourage scalable data sharing and to allow a set of secret keys to be revealed, Key-Aggregate Cryptosystem (KAC) has been introduced. In this approach, among the files which can be accessed, the secured files exempted from the set remain confidential and effective. The performance is highly boosted as the pairings are reduced. While sharing a different set of files with different people this approach declines to be flexible.

In [23], a resource efficient authentication scheme is proposed for remote users in Internet Of Things (IOT), to achieve authentication for remote users. This facilitates the network entities and users for establishing private session keys. This in turn provides indecipherable communication among the users and network entities. The proposed approach provides enhanced security against a variety of malicious attacks by providing informal security analysis. The authenticated encryption of data for resource efficiency is not concentrated in this work and this requires further analysis.

In [24], an intelligent security is introduced for processing large-scale data with the adopting of column-based approach. This approach provides improved security generating reduced impact on the data processing performance. In this work, the personal data is masked and the sensitive data is encrypted by splitting it into various parts with relevant to the sensitive level. This approach provides security with reasonable computation time and prevents cloud provider to break complete data record during decryption. Anyway, this approach did not consider various types of security levels for healthcare classification.

A modular encryption standard dependent on security measures with layered modeling is introduced in [25] to provide security in requirement-oriented health information. The approach provides auxiliary qualitative security ensuring measures along with improved performance and also restricts unwanted attempt to access data. It also ensures the data confidentiality against any malicious outsider or hackers. In spite of these advantages, the proposed work concentrates only on textual data.

3 Proposed ANN Crypto System

Analogizing with the traditional management system, cloud-based data storage is given high preference because it has a remote storage system and centralized computing power. In today's life, the medical field generates almost 10 terabytes of digitalized data. The most sensitive data are ECG reports, angiograms, and Computed Tomography (CT) scan report. These data should be secured at a high level. In this paper, three common challenges are identified and need to be addressed. Security issues, privacy challenges, and time consumption of uploading the health care data are the three prime challenges mentioned. To tackle all these issues, the ANN and Lagrange interpolation method are employed in this work for secured key generation. The first part is to identify whether the data is significant or not. To analogize between significant and insignificant data, ANN is applied. Initially, the stored data is transformed into binary format 0's and 1's. ANN analogizes by obtaining the binary value and the value in the hidden layer. The output obtained by the subtraction operation is in the form of 0's and 1's in which 0 represents the insignificant data and 1 represents the significant data. If the significant data is obtained, then it should be kept secured by generating a key with the help of Lagrange's method. The key is generated automatically by using Lagrange method and the generated key is stored in the hidden layer of ANN. So ANN plays a prominent role in this proposed work. On request for any information such as an angiogram, MRI report from the server, easy downloading of information without the knowledge of the owner is not possible. Hence, the user forwards a request message to the owner of the data through gamil. The block representation of the introduced approach is evidently illustrated in Fig. 2.

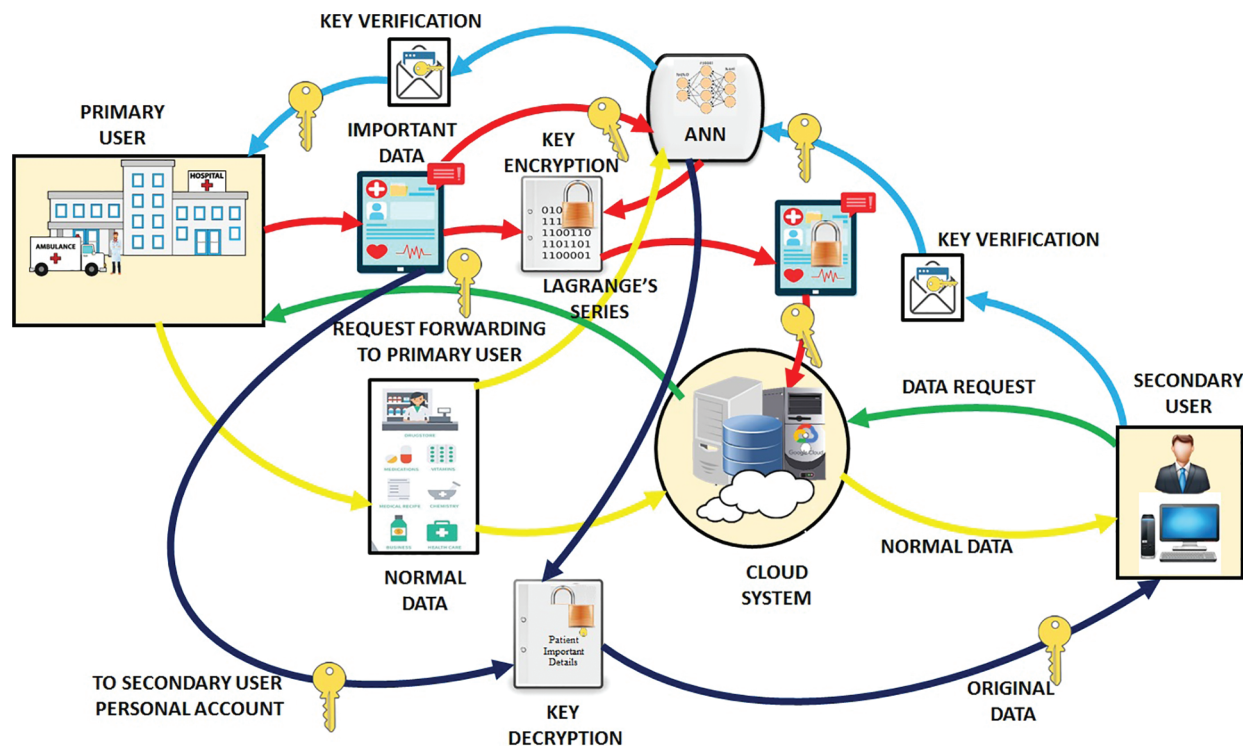


Figure 2: Block diagram of the proposed approach

If the user is known to be authenticated, the key will be forwarded to the requested client. If the key matches with the key in the hidden layer, the requested client can download the information. This

proposed work achieves security and reduced time consumption of uploading information by using ANN. As ANN has its internal memory, it speeds up the process and avoids trafficking.

4 Analogizing With Existing Cryptographic Techniques

In the existing works, public-key encryption approaches are used to uphold the incognito of healthcare information in the cloud. The drawback of these approaches are that it permits the cloud service provider to decrypt the sensitive healthcare data which may cause insecurity in turn. But in our work, it re-encrypts the encrypted text and issues key to the users requesting access to the data. The content key encryption approach is followed in other existing works. It permits the retrieval of the data by the users with a lawful license. Still the major drawback in using this technique is that it grants permission to access rights based on user's identities. In this proposed work, this problem can be handled easily by the users to access the data. The proposed approach here overcomes this problem because of the key generation and the apt usage of generated key which is shared to different types of users. Only the authorized users can have the key enabling the decryption of information. Fuzzy logic used in some works has the major drawback of using external memory to perform the operations. If any information is to be uploaded at top speed, it cannot support in such kind of situation. So this approach employs ANN which facilitates the sharing and uploading at high speed.

4.1 Artificial Neural Network in Cloud Computing Security

In this proposed work, ANN plays a prominent role and has an internal memory to process the data efficiently. In today's life, people prefer the most efficient and fastest method to obtain any information from the server. ANN tackles this demand and detects whether the information stored in the cloud is significant or not. In ANN, a neuron acquires the input from various sources and it performs certain operations to generate the output. To perform this process, it inherits four basic components.

Four basic components are,

- Accepts input.
- Process the inputs.
- Turn the processed input into an output.
- Electrochemical contact between neurons.

In ANN, each layer is interconnected and has a rudimentary structure where a few neurons "interact" with an outside source to obtain the inputs. After obtaining the input, it performs some mathematical operation between the input and hidden layers and the obtained result is transferred to the output layer. Layers of ANN is shown in [Fig. 3](#)

In the proposed work, the foremost step is to identify whether the medical-related information stored in the cloud is significant or not. This proposed work follows a hybrid pattern and in the cloud, sensitive and non-sensitive data are analyzed and kept accordingly in a private, public, and hybrid cloud. Hybrid is nothing but both public and private. In the private cloud, personal health records such as angiogram, Magnetic Resonance Imaging (MRI), and ECG reports are kept very secure. The data which are not considered as too sensitive is kept in the public cloud. To analogize between these data, ANN is applied. ANN performs this operation by obtaining the input in the form of 0's and 1's and it takes the value in the hidden layer. While training the data, if the data found in the cloud is personal, the value in the hidden layer will not be assigned. Automatically, the hidden layer takes the value as '0s' and the input value will be 1's. For example, the value in the input layer is 1111 and the value in the hidden layer is 0000. By performing a subtraction operation, it generates the output as 1111. If the obtained output is '1' then it indicates that the stored information is significant whereas '0' represents an insignificant data. In this

work, ANN performs a lateral inhibition technique. When the result is needed in terms of values in the output layer this technique is followed and it is applied in the output layer. After detecting the data, an encryption technique has to be performed. If the data is found to be a personal health record, a key has to be generated to preserve the information from the third party and the key is generated by using Lagrange's interpolation method. Further, the generated key is stored in the hidden layer of ANN. It obtains the key via the input layer from the requested client and it identifies whether the key matches with the key in the hidden layer. If it matches, it shows the result through the output layer. The interconnection between these layers has a great influence over the operation.

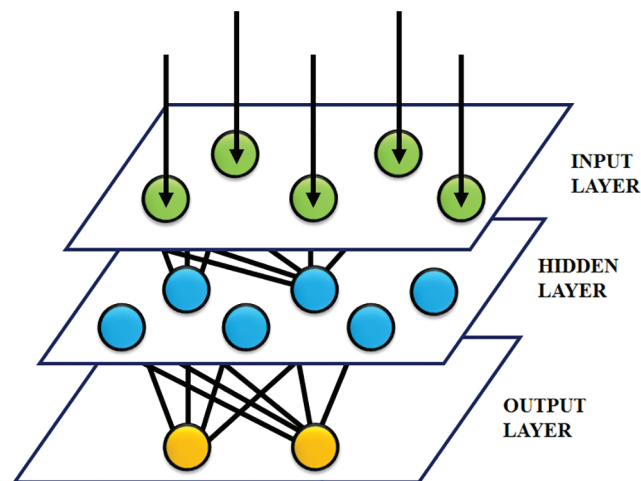


Figure 3: Layers in ANN

4.1.1 Feedforward Neural Network

The present work has proposed a security technique that could be amalgamated on various clouds. This work contains significant components, in which the transmission of information over the network is monitored, retrieved and analyzed to detect malicious behavior. The obtained information is forwarded to the feed-forward network. It integrates a feed-forward network and encryption system and its operation is done as follows. It is initially shifted to the user's machine and an activation operation takes place to generate the result. This approach does not permit to retrieve user's significant data and it is intact against malicious attack. In other existing works, cryptographic techniques are implemented. In total, 32 cryptographic keys have been used. Alternately putting these 32 keys, the personal health records can be easily downloaded from the server. In this current work, the key used is in 128 bit (2128 bits) and the tracking of key is highly complicated.

4.1.2 Secret Key Generation Using Lagrange Polynomial

The present work demonstrates the generation of secret key adopting Lagrange interpolation and the flow chart of this approach is clearly portrayed in Fig. 4. A minimum threshold number of nodes is used in the cluster with modulo arithmetic in Lagrange based approach.

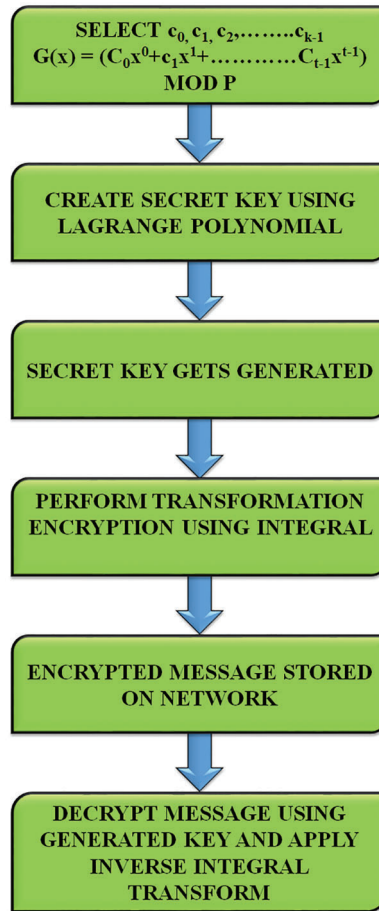


Figure 4: Flowchart

STEP 1: Generation of key

Consider $GF(p)$ indicating a polynomial equation

Select C_0, C_2, \dots, C_{k-1}

$$G(x) = (C_0X^0 + C_1X^1 + \dots C_{t-1}X^{t-1}) \text{ mod } p$$

Here, $G(0) = C_0$

Further, the partial key is provided to the sign-in id.

$$S_i = F(id_i) \tag{1}$$

Using Lagrange interpolation the polynomial is computed as follows,

$$F(x) = \sum_{i=1}^k y_i \pi_{1 \leq j \leq k, j \neq i}$$

$$= \frac{x - x_j}{x_i - x_j} \tag{2}$$

If $G(0) = C_0 = S$, the shared key is indicated as,

$$K = \sum_{i=1}^k D_i Y_i \tag{3}$$

$$D_i = \prod_{1 \leq j \leq k, j \neq i} \frac{x_j}{X_j - X_i} \tag{4}$$

Using a minimum threshold, the secret key is created as,

$$F(0) = a_0 \text{ mod } p = \text{secret key}$$

STEP 2: Encryption

The Integral transformation is used for performing encryption which provides protection for medical-related data. Considering $0 \leq t < \infty$, the integral function is given by,

$$L\{f(t)\} = F(s) = \int_0^\infty f(t)e^{-st} dt. \tag{5}$$

$$L^{-1}\{F(s)\} = f(t) \tag{6}$$

Here L^{-1} represents the inverse integral transform.

The conditions satisfied by the linear integral transformation is given by,

$$1. L\{f(t) \pm g(t)\} = L\{f(t)\} \pm L\{g(t)\} \tag{7}$$

$$2. L\{d_1 f(t)\} = d_1 L\{f(t)\} \tag{8}$$

Here, d_1 indicates a constant.

To provide security and confidentiality in data transfer, integral transformation is done in the proposed work.

A	B	C	D	-	-	Z
0	1	2	3	-	-	25

Using exponential function,

$$e^{kx} = 1 + \frac{kx}{1!} + \frac{(kx)^2}{2!} + \frac{(kx)^3}{3!} + \dots, \tag{9}$$

K denotes a real number.

Multiplying by x on both sides,

$$xe^{kx} = x \left(1 + \frac{kx}{1!} + \frac{(kx)^2}{2!} + \frac{(kx)^3}{3!} + \dots \right), \tag{10}$$

$$xe^{kx} = x1 + \frac{kxx}{1!} + \frac{x(kx)^2}{2!} + \frac{x(kx)^3}{3!} + \dots, \tag{11}$$

K indicates the Lagrange secret key.

Considering a normal text,

$$f(x) = px e^{kx} = p0x1 + p1 \frac{kxx}{1!} + p2 \frac{x(kx)^2}{2!} + p3 \frac{x(kx)^3}{3!} + \dots, \tag{12}$$

$$pxe^{kx} = x \left(p_0 1 + p_1 \frac{kxx}{1!} + p_2 \frac{(kx)^2}{2!} + p_3 \frac{(kx)^4}{3!} + \dots, \right) \tag{13}$$

$$f(x) = \sum_{n=0}^{\infty} \left(pn \frac{2^n x^{n+1}}{n!} \right)$$

Integrating on both sides,

$$L\{f(x)\} = L\{Pxe^{kx}\} = L\left\{ x \left(p_0 1 + p_1 \frac{kxx}{1!} + p_2 \frac{(kx)^2}{2!} + p_3 \frac{(kx)^3}{3!} + \dots \right), \right\} \tag{14}$$

$$L\{f(x)\} = \left(\frac{G_0}{s_n} + \frac{G_1}{S_3} + \frac{G_2}{s_4} + \frac{G_4}{s_6} \dots \dots \dots \right) \tag{15}$$

Data encryption by modular arithmetic operation:

Two similar numbers ‘a’ and ‘b’ with their difference exactly divisible by n are denoted as

$$A = b(\text{mod}n). \tag{16}$$

$$C_i = G_i \text{ mod } 26$$

$$C_i = G_i - 26d_i$$

All d_i

where ‘i’ value ranges from 0,1,2,...n.

$C_0, C_1, C_2, C_3 \dots \dots \dots C_n$ are the encrypted text of the normal text.

STEP 3: Decryption

Mathematical computations are performed for decrypting the encrypted data and is indicated as,

$$G_i = c_i + 26d_i \tag{17}$$

where ‘i’ = 0 to n.

$$L\{f(x)\} = \left(\frac{G_0}{s_1} + \frac{G_1}{S_3} + \frac{G_2}{s_4} + \frac{G_3}{s_5} + \frac{G_4}{S_6} \right) \tag{18}$$

Use Lagrange interpolation produce session key for taking inverse transform and create $p_0, p_1, p_2 \dots p_n$.

Three phases for secured information transmission in this proposed work are given as follows.

Phase 1: Generation of secret key

- Use a random number generator for creating node id.
- Produce a secret key using node id.
- Use a fixed threshold number of node id for recreating secret key.
- Select $c_0, c_1, c_2, \dots, c_{t-1} \in GF(p)$.

$$g(x) = \left(c_0 x^0 + c_1 x^1 + c_2 x^2 + \dots + c_{t-1} x^{t-1} \right) \text{ mod } p$$

Total count of users = N;

for $(k = 0; k < t; k++)$

{

```

Id[i];
}
for (k = 0; k < t; k++)
{
cr = 1;
pr = 1;
for (m = 0; m < t; m++)
{
if (m ≠ k)
{
cr = cr * (x - id[j]);
pr = pr * (id[i] - id[j]);
g(x) = (cr/pr) * Fid[i]);
}
}
Sk = g(x) mod p;

```

Phase 2: Encryption

The actual information is transformed into an alternative form named ciphertext in this process. The information can be deciphered and accessed only by authorized parties. Encryption denies the intelligible content as interceptor and does not prevent interference by itself. The information can be decrypted very easily without possessing the key. In contrast, a well-designed encryption technique is followed in this work which requires considerable computational resources and skills. The representation of this process is illustrated in Fig. 5 in an efficient manner.

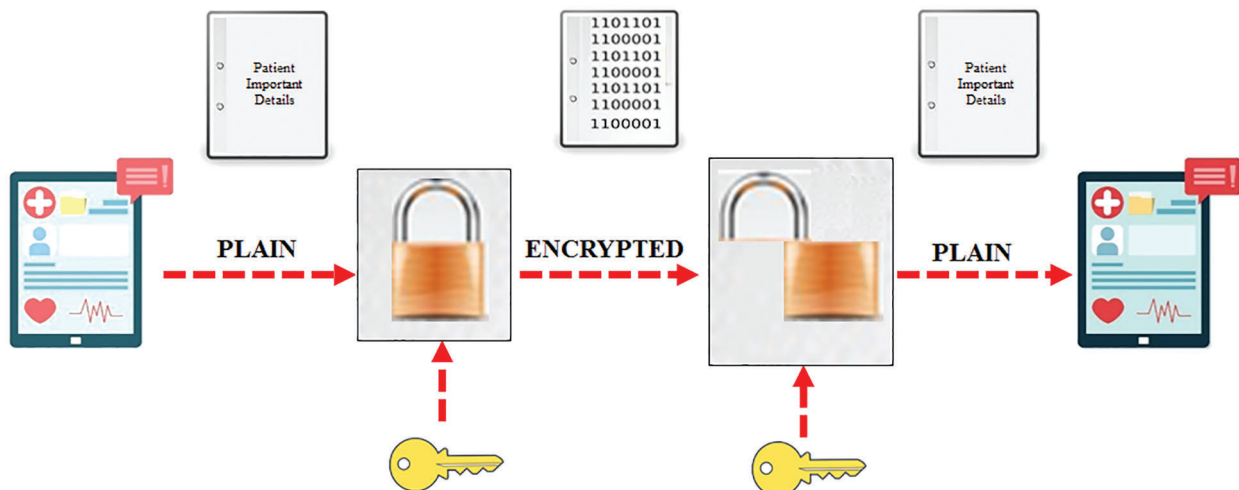


Figure 5: Encryption

- A secret key gets generated using Lagrange polynomial.
- To encrypt the information, the generated key is used in integral transform.
- The encrypted data is finally generated.

Phase 3: Decryption

The original data is retrieved in this process.

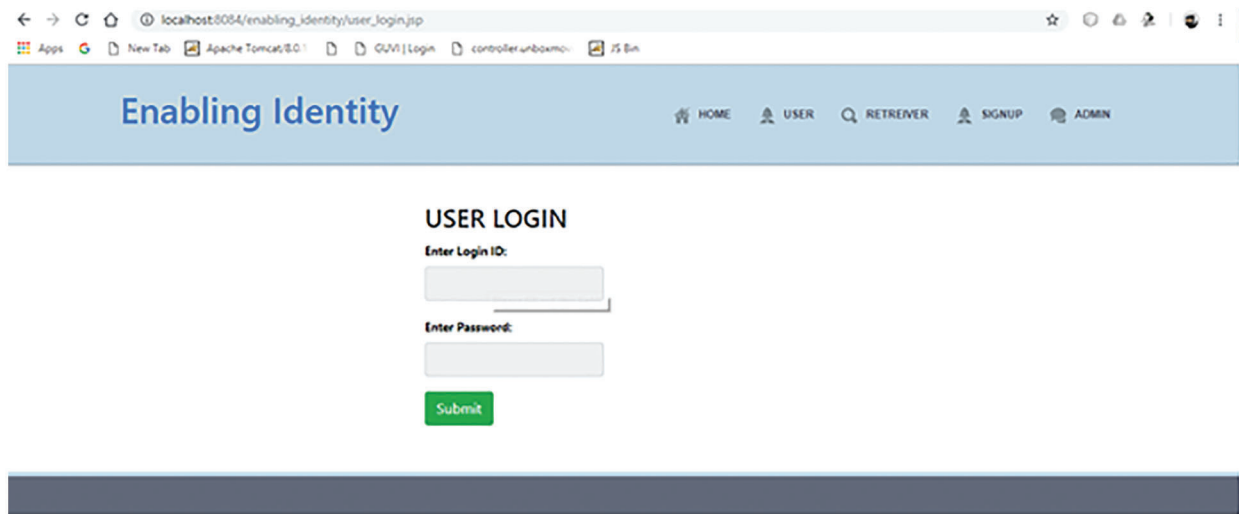
- Create a secret key by using shared partial information.
- Decrypt the message back to the original information using inverse integral.

5 Results and Discussion

In this paper, the privacy enhancement of 128-bit Lagrange interpolation based key generation is done by artificial neural network. MIT-BIH dataset is used as input data of cloud and the approach is simulated in Netbeans software.

5.1 Enabling Identity

To enable the identity, initially the user has to login by using the login id and password as represented in Fig. 6.



The screenshot shows a web browser window with the address bar displaying 'localhost:8084/enabling_identity/user_login.jsp'. The browser tabs include 'New Tab', 'Apache Tomcat/8.0', 'GUV | Login', 'controller.unboamc', and 'JS Bin'. The page header features the title 'Enabling Identity' and a navigation menu with icons and labels for 'HOME', 'USER', 'RETRIEVER', 'SIGNUP', and 'ADMIN'. The main content area is titled 'USER LOGIN' and contains a form with two input fields: 'Enter Login ID:' and 'Enter Password:'. A green 'Submit' button is positioned below the password field.

Figure 6: User login

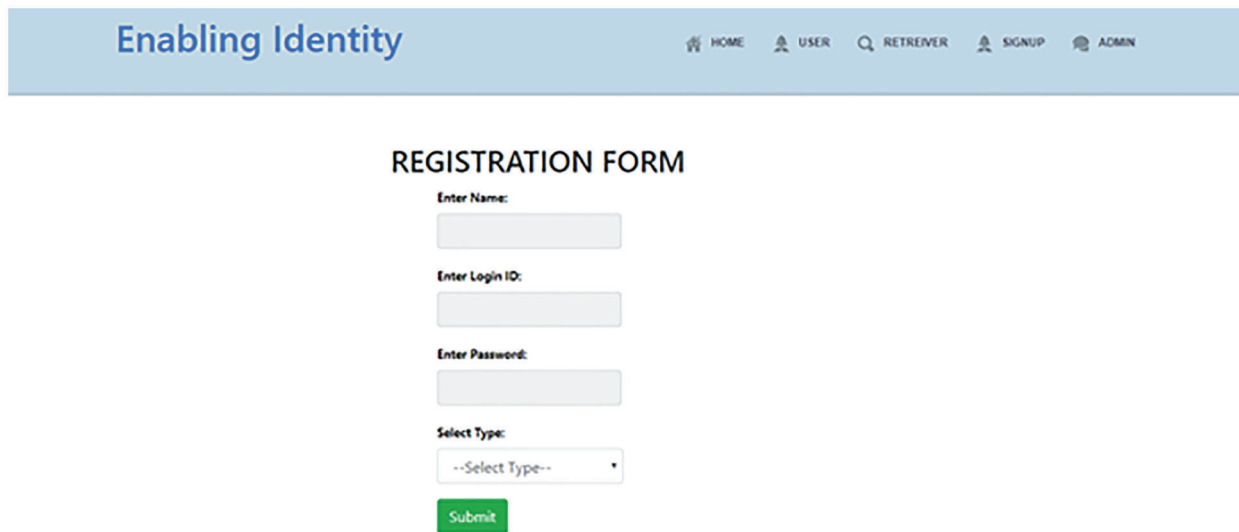
After login, the registration form appears, which is depicted in Fig. 7. In the registration form, the user has to fill in the information such as name, login id, and password.

The portal for retriever login is shown in Fig. 8. The retriever has to enter his/her login id and password.

5.2 Portal for Admin Login

The admin login page is clearly illustrated in Fig. 9 in an optimal manner.

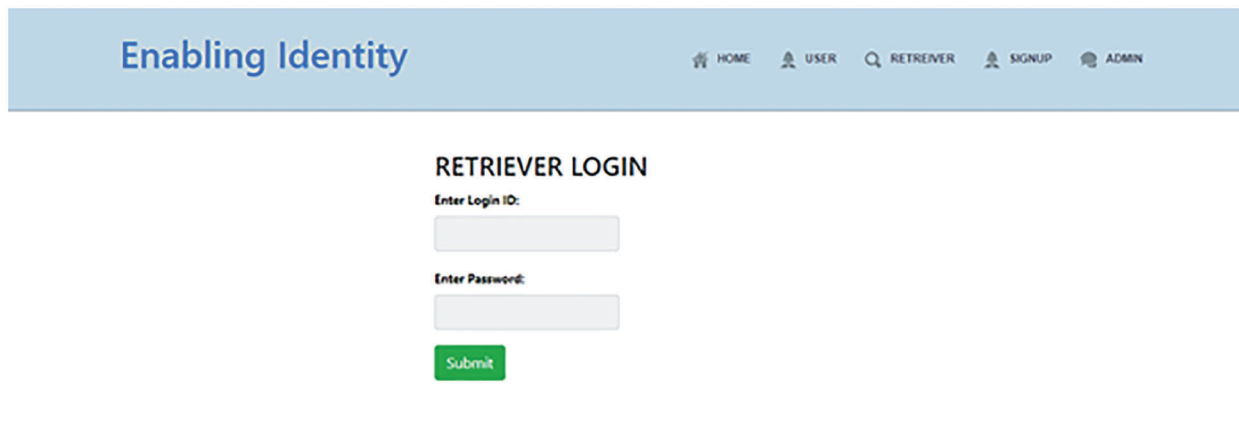
After the login process over, Key generation is performed. 128 private key gets generated by clicking the button. As the generated key is 2128 bit, cracking the key is impossible for the hackers. It is clearly portrayed in Fig. 10.



The screenshot shows a web page titled "Enabling Identity" with a navigation bar containing links for HOME, USER, RETRIEVER, SIGNUP, and ADMIN. The main content area is titled "REGISTRATION FORM" and contains the following fields:

- Enter Name:
- Enter Login ID:
- Enter Password:
- Select Type:
- Submit:

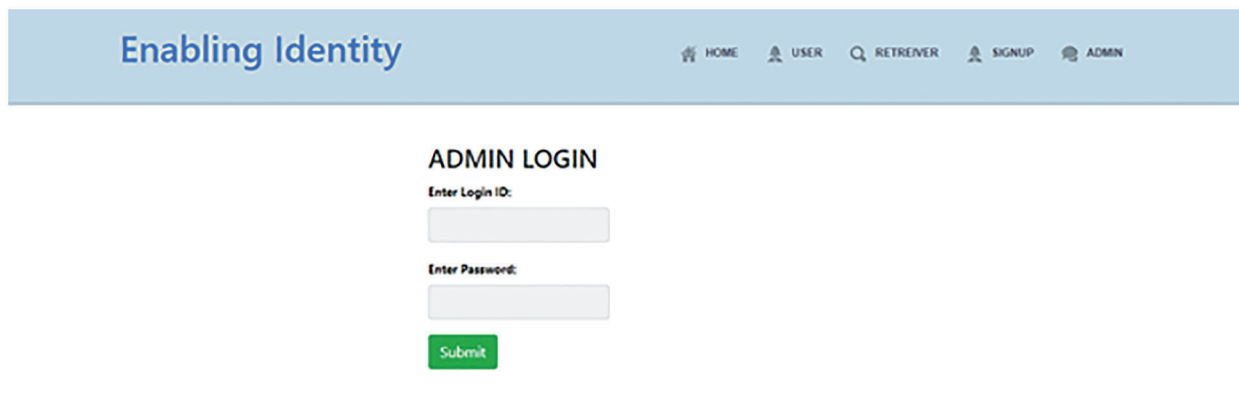
Figure 7: Registration form



The screenshot shows a web page titled "Enabling Identity" with a navigation bar containing links for HOME, USER, RETRIEVER, SIGNUP, and ADMIN. The main content area is titled "RETRIEVER LOGIN" and contains the following fields:

- Enter Login ID:
- Enter Password:
- Submit:

Figure 8: Retriever login



The screenshot shows a web page titled "Enabling Identity" with a navigation bar containing links for HOME, USER, RETRIEVER, SIGNUP, and ADMIN. The main content area is titled "ADMIN LOGIN" and contains the following fields:

- Enter Login ID:
- Enter Password:
- Submit:

Figure 9: Admin login

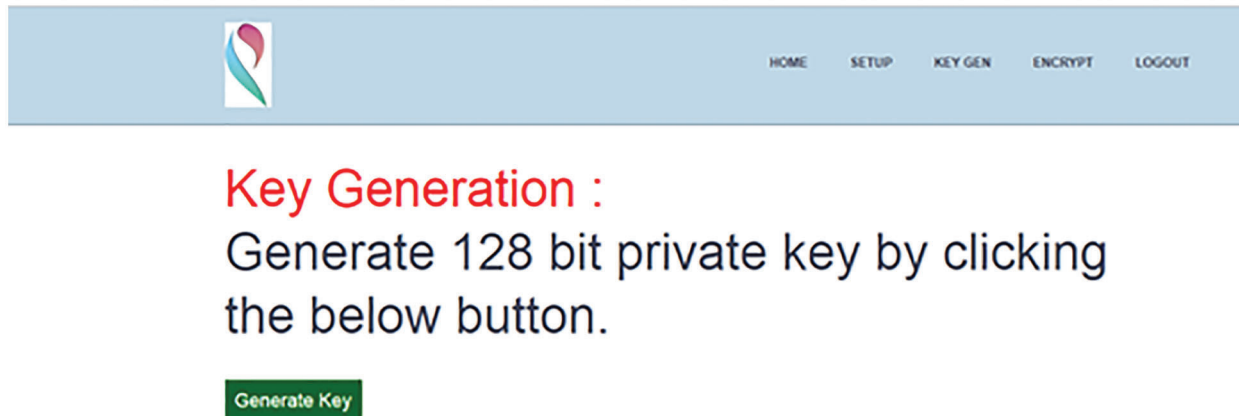


Figure 10: Key generation

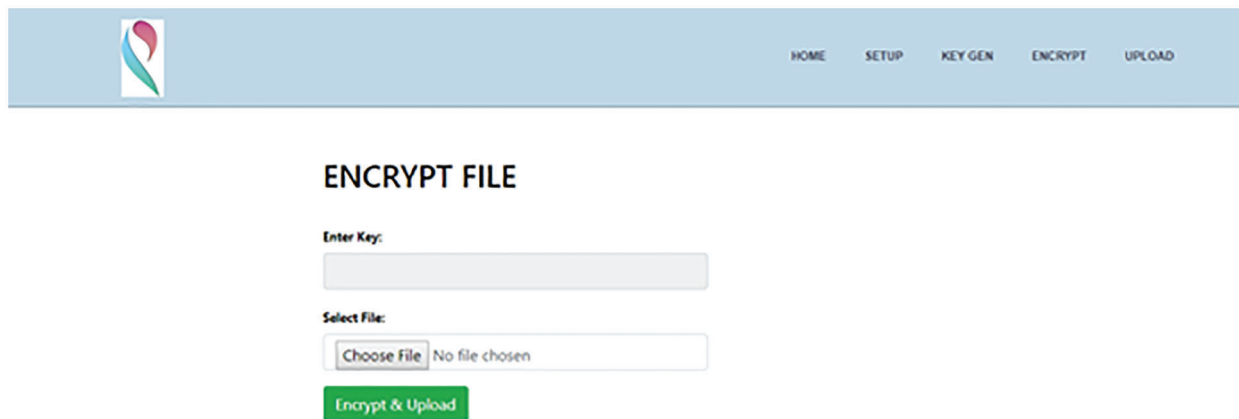


Figure 11: Encrypted file

5.3 Encryption

To encrypt the file, the key has to be entered as represented in Fig. 11. If the key matches with the key in the hidden layer of ANN the requested user can upload the needed data.

5.4 Decryption

To decrypt the ciphertext, the secret key which is shared already has to be entered and the content has to be changed back to its normal form as depicted in Fig. 12.

5.5 Performance Metrics

The graphs in Figs. 13 and 14 clearly show the duration of time to generate the key. While multiple users access the information from the cloud, it generates a key in a short interval of time. This proposed work works well in achieving time consumption of generating a key to encrypt and decrypt the message.

Time consumption for encryption and decryption indicates that the gradual increase of the time is depending upon the file size and it shows that it consumes less time in performing this operation. Figs. 15 and 16 significantly illustrate the time consumption of encryption and decryption.

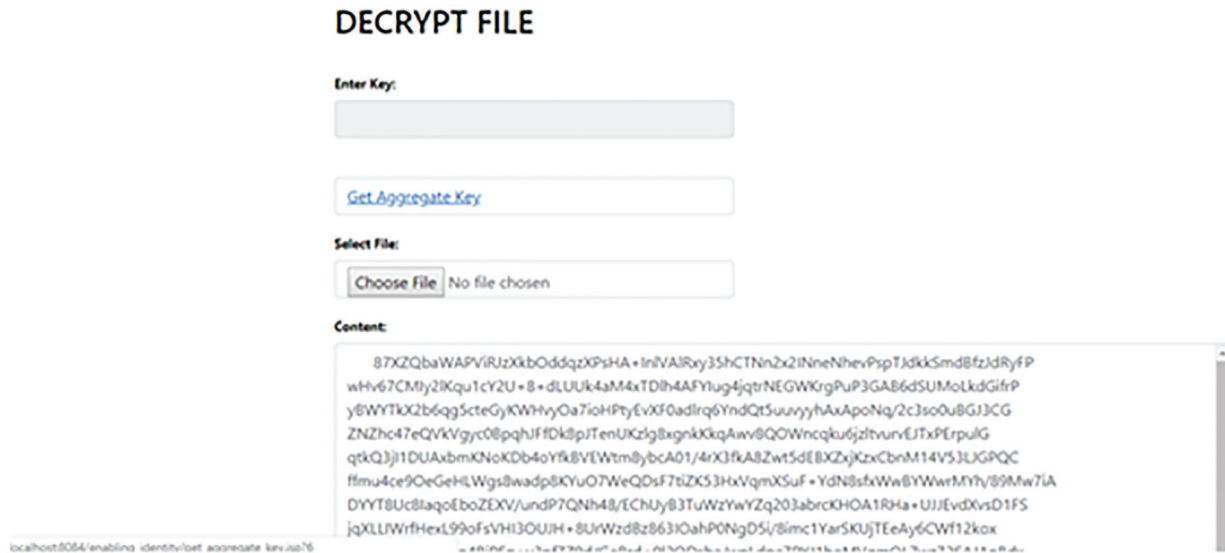


Figure 12: Decrypted file

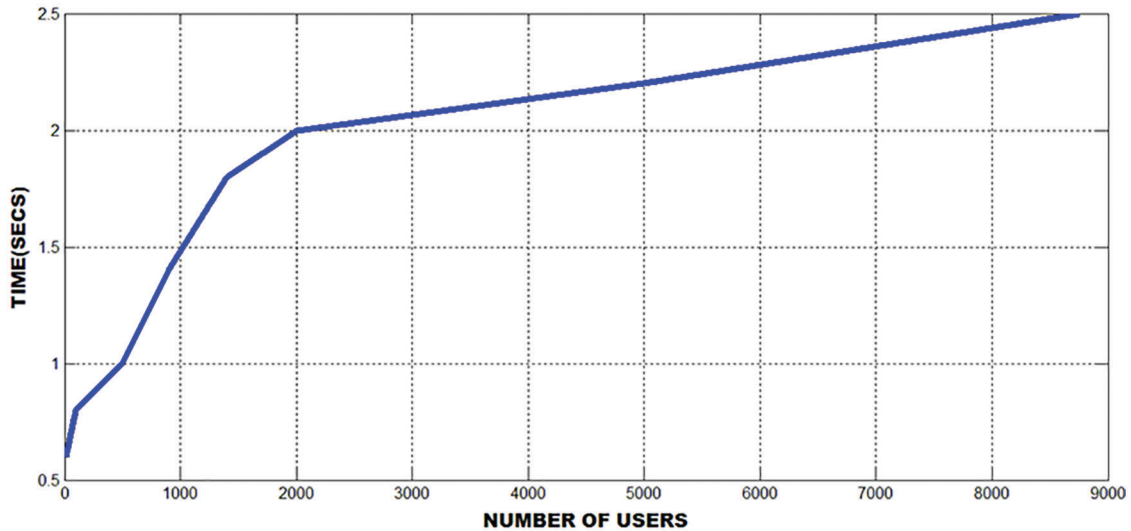


Figure 13: Time taken for creating a key

The demonstration of the SeSPHR scheme is also validated with [14] and [25] by concerning its turnaround time related to encryption and decryption, which is significantly depicted in Fig. 17. Turnaround time for encryption is computed using,

$$T_{T-up} = t_{Enc} + t_{up} \tag{19}$$

where t_{enc} and t_{up} denotes the encrypted time

Turnaround time for decryption is computed by using the equation,

$$T_{t-down} = t_{dec} + t_{down}. \tag{20}$$

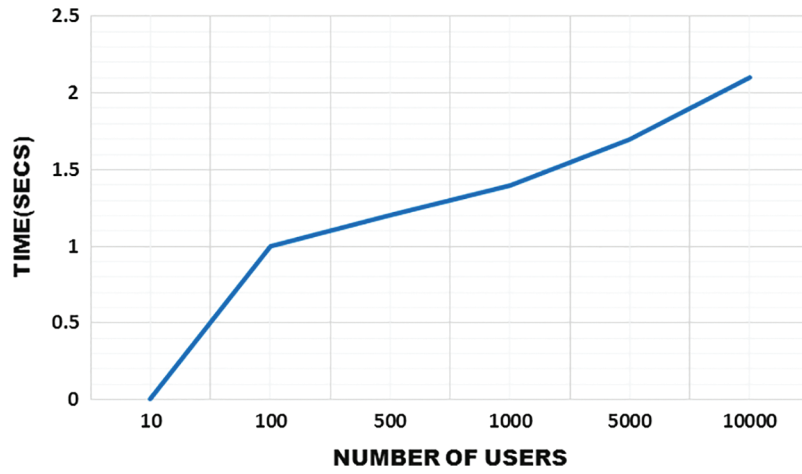


Figure 14: Time taken for creating a key

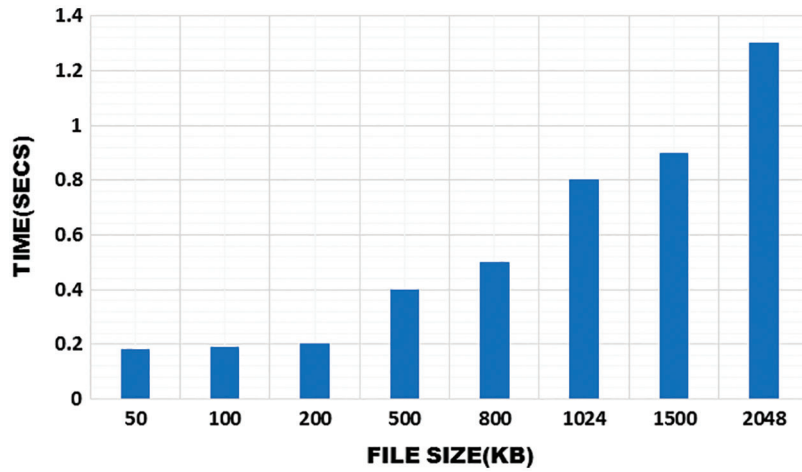


Figure 15: Time to perform encryption

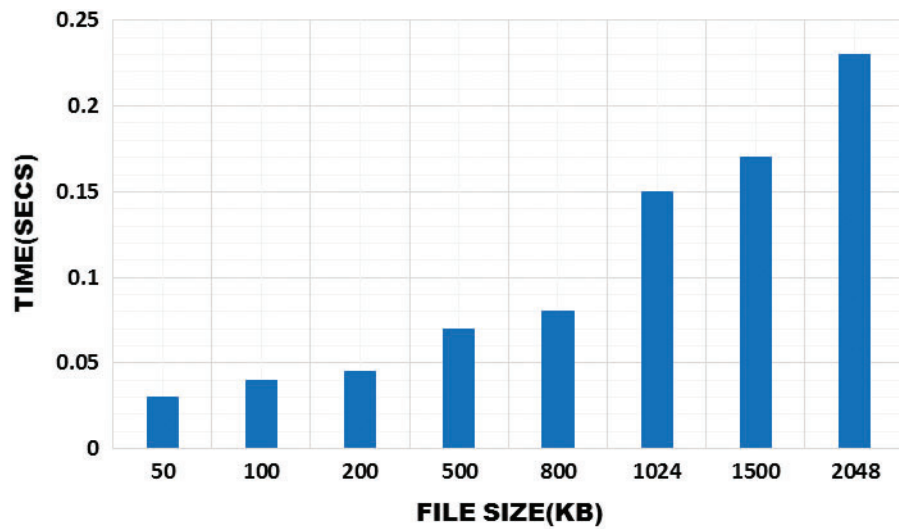


Figure 16: Time to perform decryption

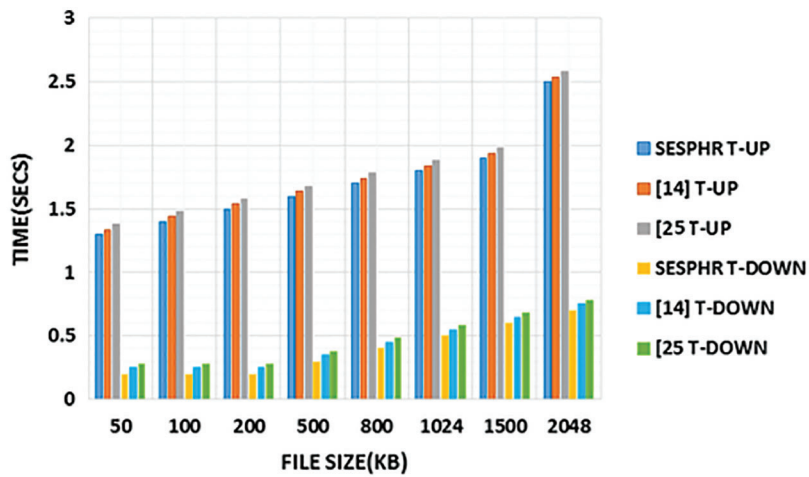


Figure 17: Comparison of turnaround time eSPHR with [14] and [25]

Here, ANN secures the highest score, once the requested user can retrieve the service preference of its client quickly, it can satisfy the user at a top-notch. The initial thing to be concerned about is the decision threshold of gratification which performs detecting whether a transaction is favorable or contradictory. The lower threshold gains a high-level of achievement in analogizing the rate and satisfaction. Conversely if there is over time for a higher threshold, then some precise resource classification condition will be performed and the success rate and satisfaction get raised steadily. However, when the user prefers the gradual raise from low to high, the influences of the different transaction threshold will be steadily approaching within the given amount of time. The graphs representing the comparison outcomes of convergence ratio and user satisfaction are evidently depicted in Figs. 18 and 19.

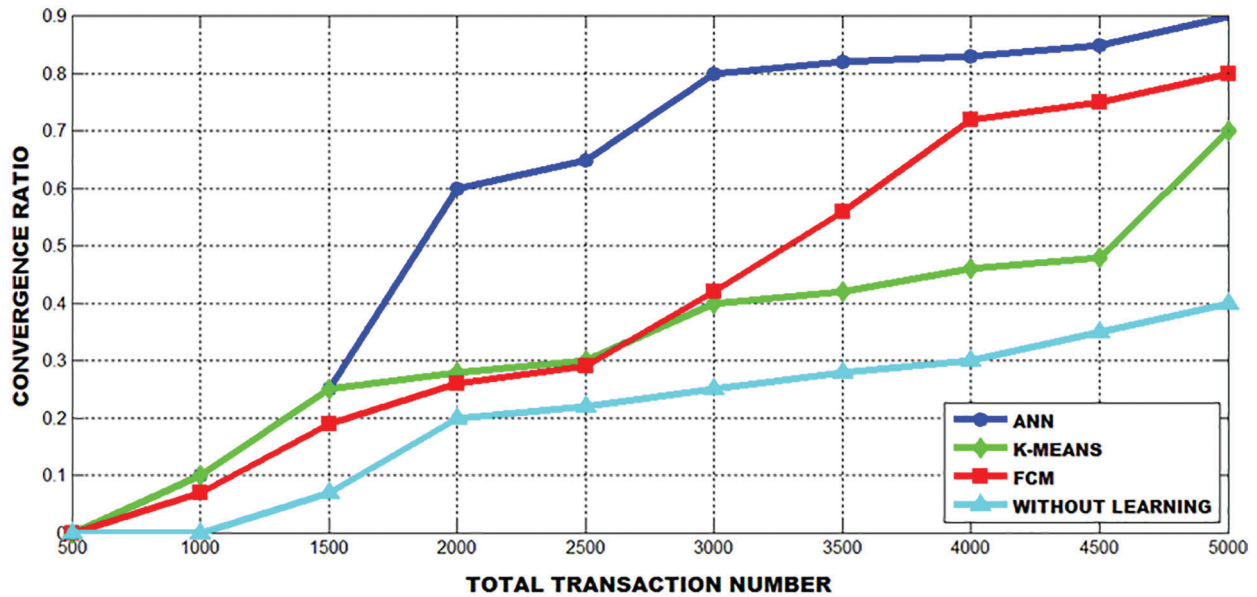


Figure 18: The comparison of convergence ratio

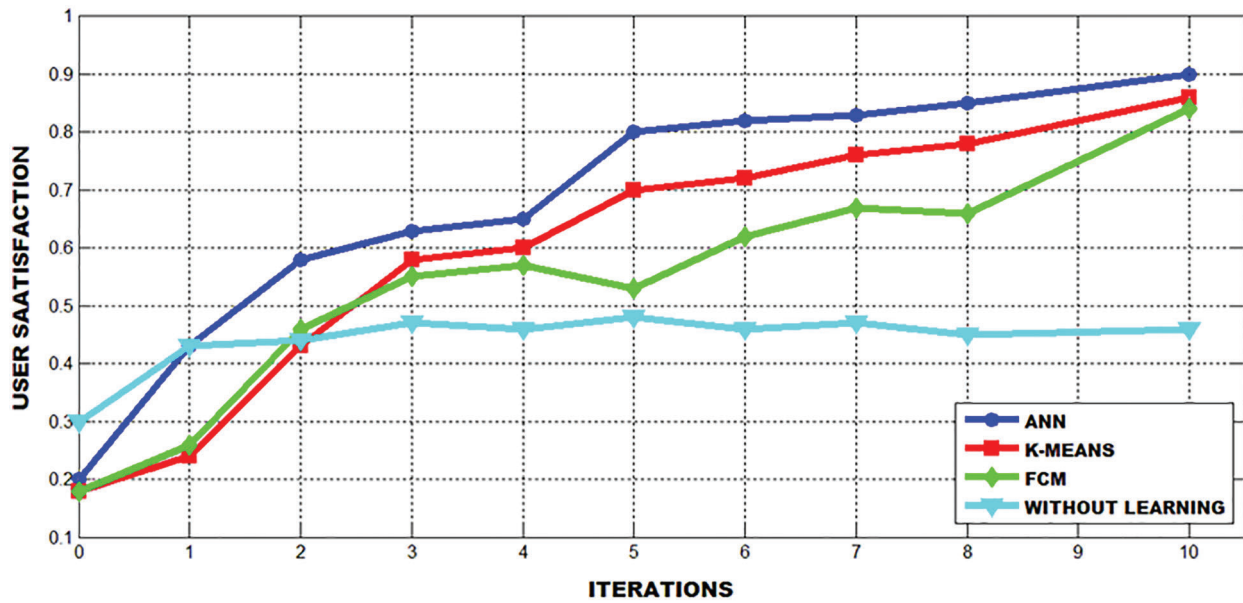


Figure 19: The comparison of user satisfaction

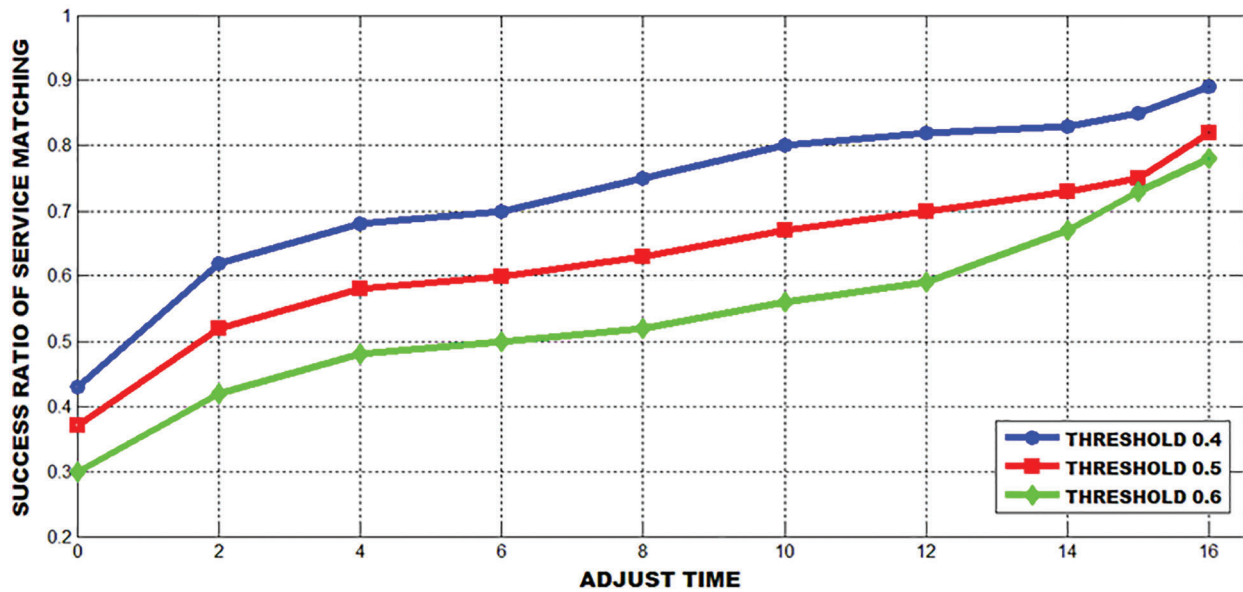


Figure 20: A success ratio of service matching based on the different decision threshold

Figs. 20 and 21 show the effect of various decision factors in the success ratio of service matching in an optimal manner.

The graph in Fig. 22 clearly indicates that the ratio of success is relatively exaggerated though there is a larger number of felonious users.

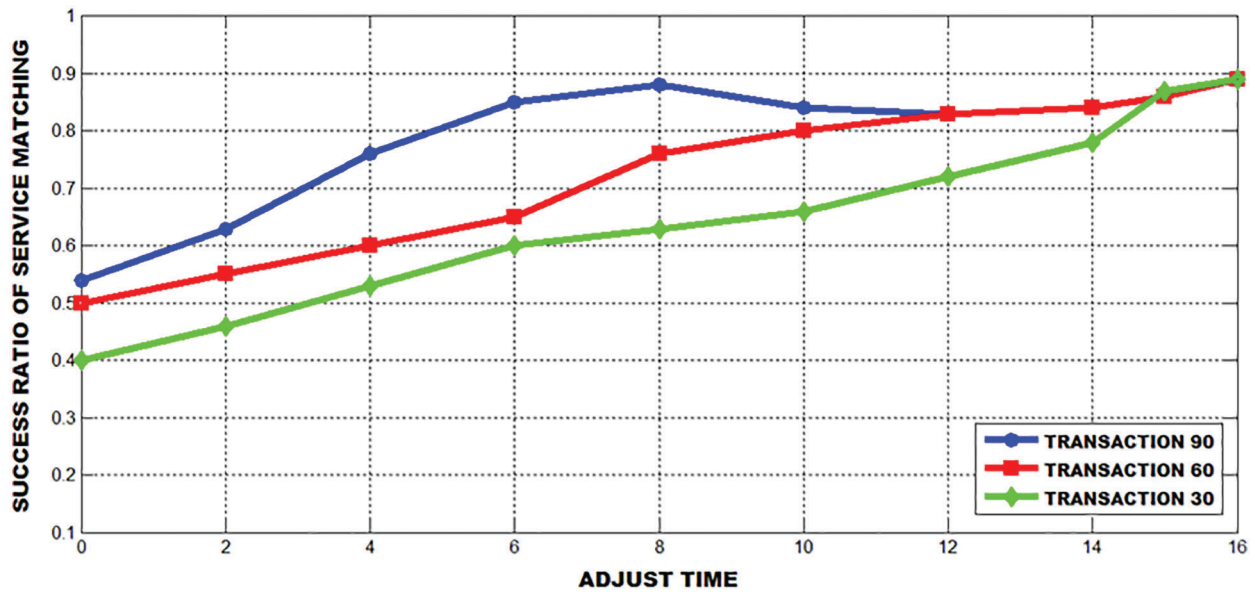


Figure 21: A success ratio of user satisfaction

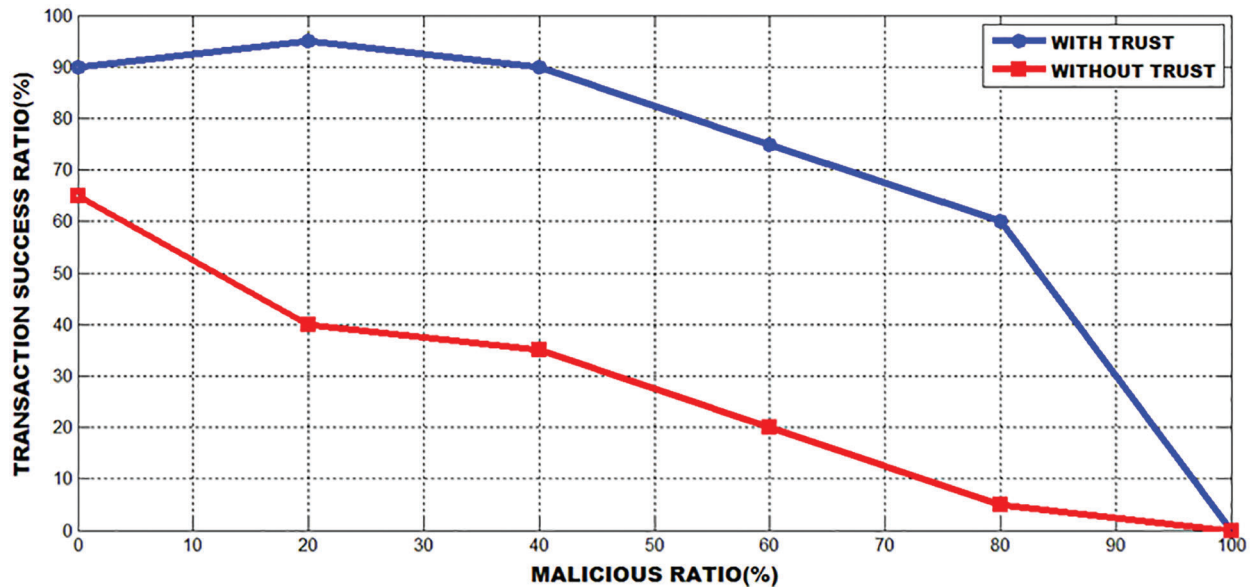


Figure 22: The effect of trust on transaction ratio of success

6 Conclusion

Nowadays, smart healthcare services provide a great asset and it is dominantly used by health care organizations. The health care data stored in the cloud, is highly susceptible to threats and breaches. So a high level security is essential to safeguard the data from unauthorized users. The present work proposes an advanced framework for cloud services. This advanced framework has the proficiency to improve the cloud security which shares the health care data over the network. The proposed algorithm achieves high security and protection by using Lagrange polynomial for the generation of secret key which performs the encryption and decryption. The main advantage of using Lagrange is that it generates the key

automatically without any interference thus preventing tracking by hackers. ANN performs effective classification of data based on its significance improving privacy and security. This proposed cloud based mechanism results in enhanced success rate, convergence ratio and user satisfaction indicating efficient security and privacy preserving in health care data.

Funding Statement: The authors received no specific funding for this study.

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

References

- [1] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu *et al.*, “An efficient protocol with bidirectional verification for storage security in cloud computing,” *IEEE Access*, vol. 4, pp. 7899–7911, 2016.
- [2] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun *et al.*, “Block design-based key agreement for group data sharing in cloud computing,” *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996–1010, 2019.
- [3] W. Liu, P. Wang, Y. Meng, Q. Zhao, C. Zhao *et al.*, “A novel model for optimizing selection of cloud instance types,” *IEEE Access*, vol. 7, no. 8, pp. 120508–120521, 2019.
- [4] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang *et al.*, “Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach,” *IEEE Access*, vol. 7, pp. 9368–9383, 2019.
- [5] I. S. B. M. Isa, T. E. H. El-Gorashi, M. O. I. Musa and J. M. H. Elmirghani, “Energy efficient fog-based healthcare monitoring infrastructure,” *IEEE Access*, vol. 8, pp. 197828–197852, 2020.
- [6] M. Akter, A. Gani, M. O. Rahman, M. M. Hassan, A. Almogren *et al.*, “Performance analysis of personal cloud storage services for mobile multimedia health record management,” *IEEE Access*, vol. 6, pp. 52625–52638, 2018.
- [7] K. Riad, R. Hamza and H. Yan, “Sensitive and energetic IoT access control for managing cloud electronic health records,” *IEEE Access*, vol. 7, pp. 86384–86393, 2019.
- [8] H. Qiu, M. Qiu, M. Liu and G. Memmi, “Secure health data sharing for medical cyber-physical systems for the healthcare 4.0in,” *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 9, pp. 2499–2505, 2020.
- [9] S. Sengupta and S. S. Bhunia, “Secure data management in cloudlet assisted IoT enabled e-health framework in smart city,” *IEEE Sensors Journal*, vol. 20, no. 16, pp. 9581–9588, 2020.
- [10] Q. Zhang, Q. Zhang, W. Shi and H. Zhong, “Firework: Data processing and sharing for hybrid cloud-edge analytics,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 29, no. 9, pp. 2004–2017, 2018.
- [11] A. Nhlabatsi, J. B. Hong, D. S. Kim, R. Fernandez, A. Hussein *et al.*, “Threat-specific security risk evaluation in the cloud,” *IEEE Transactions on Cloud Computing*, vol. 9, no. 2, pp. 793–806, 2021.
- [12] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami *et al.*, “A systematic literature review on cloud computing security: Threats and mitigation strategies,” *IEEE Access*, vol. 9, pp. 57792–57807, 2021.
- [13] C. Meshram, C. C. Lee, A. S. Ranadive, C. T. Li, S. G. Meshram *et al.*, “A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing,” *International Journal of Communication Systems*, vol. 33, no. 7, pp. e4307, 2020.
- [14] M. Farid, R. Latip, M. Hussin and N. A. W. A. Hamid, “Scheduling scientific workflow using multi-objective algorithm with fuzzy resource utilization in multi-cloud environment,” *IEEE Access*, vol. 8, pp. 24309–24322, 2020.
- [15] P. Chinnasamy, S. Padmavathi, R. Swathy and S. Rakesh, “Efficient data security using hybrid cryptography on cloud computing,” in *Inventive Communication and Computational Technologies*, Singapore: Springer, pp. 537–547, 2021.
- [16] P. Peddi, “Data sharing Privacy in Mobile cloud using AES,” *International Journal of Scientific Research in Computer Science Applications and Management Studies*, vol. 1, no. 4, pp. 1953–2319, 2018.
- [17] J. Ni, K. Zhang, Y. Yu and T. Yang, “Identity-based provable data possession from RSA assumption for secure cloud storage,” *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 8, 2020.
- [18] S. Ambika, S. Rajakumar and A. S. Anakath, “A novel RSA algorithm for secured key transmission in a centralized cloud environment,” *International Journal of Communication Systems*, vol. 33, no. 5, pp. e4280, 2020.

- [19] Y. Yang, X. Li, N. Qamar, P. Liu, W. Ke *et al.*, “Medshare: A novel hybrid cloud for medical resource sharing among autonomous healthcare providers,” *IEEE Access*, vol. 6, no. 8, pp. 46949–46961, 2018.
- [20] H. Wang, D. He and S. Tang, “Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1165–1176, 2016.
- [21] W. Wang, P. Xu, D. Liu, L. T. Yang and Z. Yan, “Lightweighted secure searching over public-key ciphertexts for edge-cloud-assisted industrial iot devices,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4221–4230, 2020.
- [22] K. S. Babu, N. Sindhu and K. Rameshwaraiah, “Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud,” *International Journal of Recent Trends in Engineering & Research*, pp. 261–265, 2017.
- [23] G. Abbas, M. Tanveer, Z. H. Abbas, M. Waqas, T. Baker *et al.*, “A secure remote user authentication scheme for 6LoWPAN-based Internet of Things,” *PLoS One*, vol. 16, no. 11, pp. e0258279, 2021.
- [24] Y. M. Essa, E. E. D. Hemdan, A. El-Mahalawy, G. Attiya and A. El-Sayed, “IFHDS: Intelligent framework for securing healthcare bigdata,” *Journal of Medical Systems*, vol. 43, no. 5, pp. 1–13, 2019.
- [25] M. Shabbir, A. Shabbir, C. Iwendi, A. R. Javed, M. Rizwan *et al.*, “Enhancing security of health information using modular encryption standard in mobile cloud computing,” *IEEE Access*, vol. 9, pp. 8820–8834, 2021.