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

Stochastic Gradient Deep Multilayer Neural Network based Linear Congruential Generative Cryptosystem for Secured Data Communication in Cloud

Mrs. Krishnaveni R[1], Dr. Shakila S[2]
[1] Research Scholar, Government Arts College, Trichy 620022
Affiliated to Bharathidasan University, Trichy 620024
[2] Department of Computer Science, Government Arts College, Trichy 620022
Affiliated to Bharathidasan University, Trichy 620024

Abstract

Cloud computing is a kind of distributed computing that use a vast network of interconnected resources accessible over the internet. Security is a crucial concern in cloud computing due to the fact that users save their data on the cloud for convenient access from any location and at any time. Consequently, many users are worried about safeguarding their sensitive data in an unsafe location. Therefore, cloud computing architecture requires an innovative cryptographic method that ensures the secrecy, authenticity, integrity, and non-repudiation of data transfer in the cloud. A new technique called SEMcrypt, which stands for Stochastic Gradient DEep Multilayer Neural Network based Linear Congruential Generative Cryptography, has been developed to enhance secure data transmission. SEMcrypt ensures higher data confidentiality and reduces the time required for communication between the cloud user (i.e., patient) and the server. The SEMcrypt approach has two distinct processes: categorization and secure data transport. Initially, the data is gathered from the patients and is used as input for the stochastic gradient regularised deep multilayer neural network. The deep neural network consists of one input layer, two hidden layers, and one output layer. At first, the information is gathered from the patients and sent to the input layer. Next, the patient data that has been gathered is examined in hidden layer 1 using the generalised Tikhonov regularisation function. The patient data that has been analysed is sent to hidden layer 2. The hyperbolic tangent activation function is used at that layer to classify the patient data. Subsequently, the categorised data undergoes encryption via the use of Linear Congruential Generative Goldwasser-Micali encryption, ensuring safe transfer of the data. Subsequently, the encrypted data is sent to the cloud server. The patient data is encrypted on the server side using the Linear Congruential Generative Goldwasser-Micali decryption technique to prevent unauthorised access or assaults. Consequently, the authorised recipient receives the unaltered information, which is then kept in the database for further analysis. Secured data transmission is achieved by ensuring better levels of data confidentiality and reducing the time required for the process. The experimental assessment focuses on criteria such as the time it takes to generate keys, the level of data confidentiality and integrity, the computing time, and the accuracy of categorization. The empirical findings demonstrate that our suggested SEMcrypt approach delivers efficient performance outcomes by attaining superior levels of data confidentiality and integrity within a minimal timeframe.

Keywords: Cloud computing, secure data communication, stochastic gradient regularized deep multilayer neural network, generalized Tikhonov regularization function, Linear Congruential Generative Goldwasser–Micali Cryptosystem

1. Introduction

Cloud computing is a decentralised technology that offers resources and utility services in response to user requests. Hence, it is essential to have effective cloud security measures, particularly during data transmission. Privacy and security are significant considerations in the healthcare sector to safeguard patient sensitive data. In order to bolster the security and privacy of healthcare data, many techniques have been devised inside the cloud computing environment.

In [1], a resilient and efficient access protocol was proposed for E-healthcare services to prevent unauthorised users from accessing information stored on the cloud server. However, the integrity level did not see any enhancement. The Lightweight Attribute-Based Searchable Encryption (LABSE) approach, introduced in [2], aims to provide fine-grained access control and reduce the processing time required for safe data transfer. Nevertheless, the implemented strategy proved to be inadequate in ensuring security.

In [3], a hybrid cryptographic technique was proposed to address the security concerns associated with cloud computing technologies. However, it exhibits a longer computational time while addressing the security issue. In [4], two robust and effective cryptosystems were created to ensure the safe storage and retrieval of medical data. These

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

systems use the High safe Encryption Standard scheme. But it failed to apply vast amount of data.

In [5], a novel cryptographic technique was presented to ensure data security analysis with reduced computing time. A novel technique for transferring blockchain data was devised in [6], using homomorphic encryption to enhance transmission precision and reduce transmission duration.

In [7], a novel non-cryptographic technique was developed to safeguard the security and integrity of electrocardiograph (ECG) data during transmission. Nevertheless, the efficiency of healthcare data transfer was not improved. In [8], a technique called the Improved Henon Chaotic Map-based Progressive Block-based approach was proposed to enhance encryption security by preventing the disclosure of confidential data.

In [9], a Secure Quantum Key Distribution for Cloud Data Security (SQKD-CDS) technique was devised to provide data security in cloud environments. In [10], a mechanism for safe and encrypted data-sharing based on identification was created to ensure the protection of important electronic health records. However, both cryptographic and non-cryptographic techniques were not used to safeguard the confidentiality and integrity of digital data.

1.1 Contributions

To address the current challenges, a new approach called SEMcrypt is developed, which offers innovative features like,

- A new method called SEMcrypt is proposed to enhance the security of transmitting health data in the cloud. This methodology combines Linear Congruential Generative Goldwasser-Micali cryptography with a stochastic gradient regularised deep multilayer neural network.
- There is no text provided. In order to enhance the accuracy of classification and reduce the error rate, a stochastic gradient regularised deep multilayer neural network is used to categorise the patient data into distinct categories. The use of Generalised Tikhonov regularisation is used to quantify the correlation between the patient data. The hyperbolic tangent function is used to categorise patient data in order to minimise the inaccuracy.
- Linear Congruential Generative Goldwasser-Micali cryptography is implemented to enhance data security and integrity by encrypting and decrypting data, hence preventing unauthorised assaults.
- Finally, we conduct thorough experimental assessments to assess the performance of our SEMcrypt approach and compare it with existing strategies using diverse criteria.

1.1 paper outline

The remaining portion of the work is organised into six distinct parts in the following manner. Section 2 provides an overview of the relevant literature. Section 3 presents a concise overview of the suggested use of the SEMcrypt technology, accompanied by a well-organized architectural design. Section 4 details the empirical investigation conducted on the dataset description. Section 5 presents the outcomes and analyses of the proposed SEMcrypt approach and compares them with current techniques using various measures. Section 6 serves as the concluding section of the paper.

2. Related works

In [11], heterogeneous integrated network resource management strategies were created to enhance the transmission of information security. In [12], an integrated altered Paillier and KLEIN algorithms were proposed to enhance the security of patients' data storage and access. However, the desired level of secrecy was not attained. In order to enhance the security of cloud systems against assaults, a unique Two-Factor authentication mechanism was devised in [13]. A very effective and practical cloud infrastructure was presented in reference [14] to provide safe data transfer. In [15], a Confidentiality-based Classification-as-a-Service (C2aaS) was created to handle data processing while considering the degree of data security.

In [16], a unique system for managing personal health records (PHR) was created. This technique used a blockchain platform to enhance the efficiency of healthcare administration processes. In [17], a novel security-by-design methodology was devised to provide safe data transfer. However, there were no enhancements made to the security measures for data privacy protection and the integrity of data transfer.

In order to enhance the security of health information, a Modular Encryption Standard (MES) technique was proposed in [18]. However, it was unsuccessful in guaranteeing patient confidentiality using the blockchain security framework. In order to enhance integrity and reduce computation cost, proven data

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

possession (PDP) protocols were devised in [19]. In [20], a more advanced approach of revocable and identity-based conditional proxy re-encryption was presented. This method aims to enhance the security and efficiency of sharing cloud data.

3. Methodology

As a result of the progress in cloud healthcare models, a substantial volume of medical data is being communicated over the internet. The healthcare data saved in the cloud is regarded as a highly sensitive record, safeguarding against unauthorised access to patient information. Therefore, the security measures concerning the transfer of medical data via cloud-based systems are of great importance, since users upload their sensitive information and connect to the cloud to access it. However, the perpetrators often anticipate the advancements in technology and use the information via hacking. In order to ensure the security of data, the majority of systems use encryption methods that are based on specialised algorithms designed for data protection. Nevertheless, ensuring high levels of data security and integrity poses significant challenges. Hence, the development of a unique approach called SEMcrypt aims to enhance the security of transmitting medical data in cloud computing.

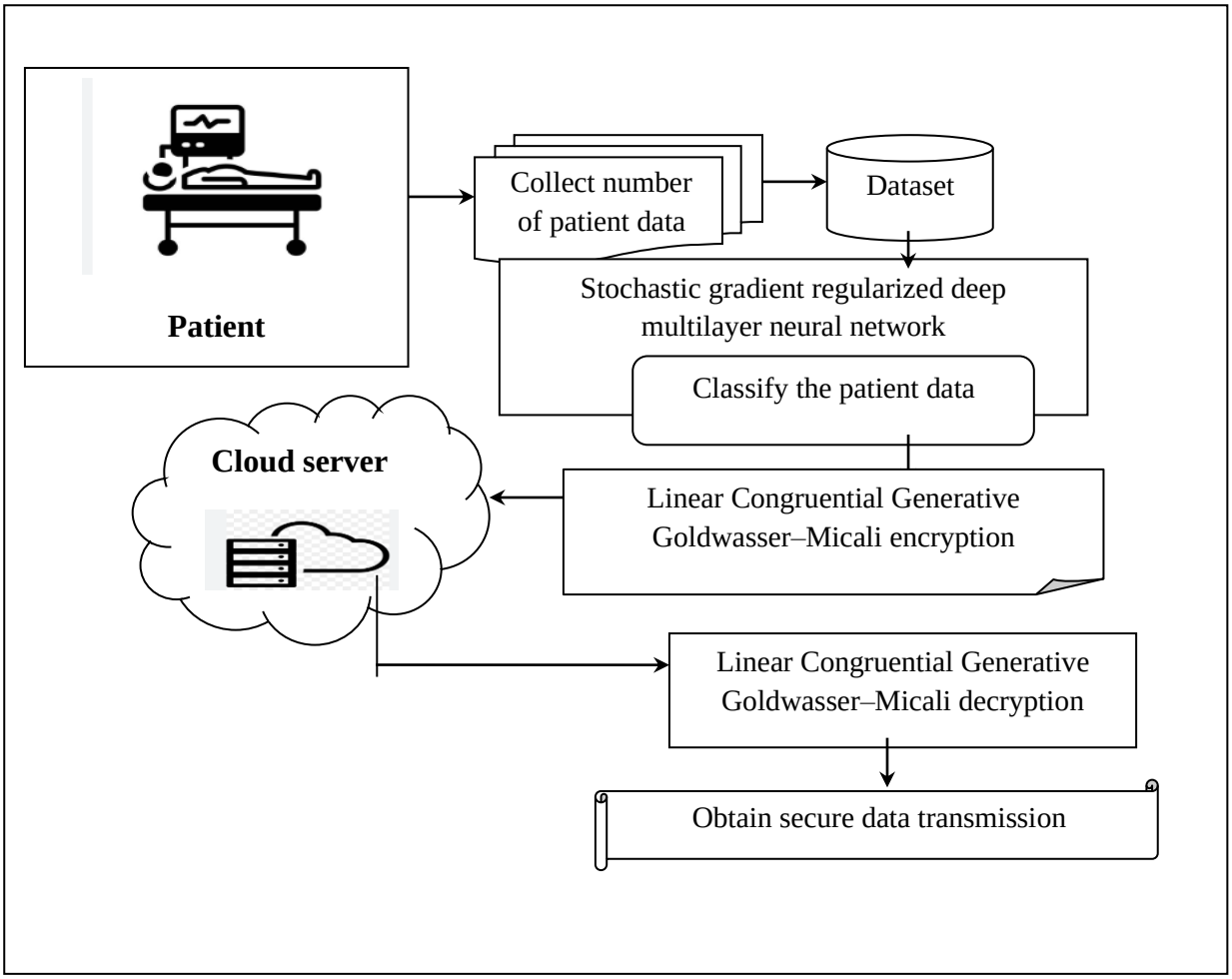

Figure 1 architecture diagram of proposed SEMcrypt technique

Figure 1 illustrates the architectural design of the SEMcrypt technology, which aims to provide secure data transfer with enhanced data confidentiality and integrity in the healthcare context. The architecture consists of two entities: users, namely patients $P_1, P_2, P_3 \ldots\ldots P_n$ who create healthcare data $pd_1, pd_2, pd_3, \ldots. pd_m$ The gathered data is securely sent to the cloud server 'CS' to facilitate the provision of suitable telemedicine services. Hence, the suggested approach for secure transmission effectively transfers medical data to the cloud server.

Prior to transmitting the data, the patient data that has been gathered is categorised using a stochastic gradient regularised deep multilayer neural network. Following the process of data categorization, the cloud user employs the Linear Congruential Generative Goldwasser-Micali encryption technique to transform the incoming patient data

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

into ciphertext. Subsequently, the encrypted data is kept inside the cloud server. Each time the user retrieves data from the server, they use the valid key to decrypt the original patient data. This is done to prevent unauthorised access and enhance the level of data confidentiality. The SEMcrypt approach is elucidated in the following subsections, which outline the two distinct procedures involved.

3.1 Stochastic gradient Tikhonov Regularized Deep multilayer Neural Network based data Classifier

The first step of the proposed SEMcrypt involves doing data categorization to minimise the time required for secure data connection in cloud computing. The suggested method employs a stochastic gradient Tikhonov regularised deep multilayer neural network to categorise the provided patient data. The deep structure multilayer neural network has the benefit of effectively managing a substantial amount of input data and achieving more precise classifications compared to other deep learning approaches.

The suggested neural network consists of an input layer, an output layer, and many hidden layers, forming a deep structure. The input layer receives the input, which corresponds to the quantity of patient data that has to be processed. The process of categorising is performed inside the concealed layer. The number of hidden layers is arbitrarily situated between the input and output layers. Each layer is often composed of minuscule individual units referred to as artificial neurons or perceptrons. Every individual neuron inside a given layer is connected to the neurons in the preceding layer, resulting in the formation of a comprehensive network architecture. A synapse denotes the interconnections among neurons. Figure 2 displays the arrangement of the proposed deep structure multilayer neural network.

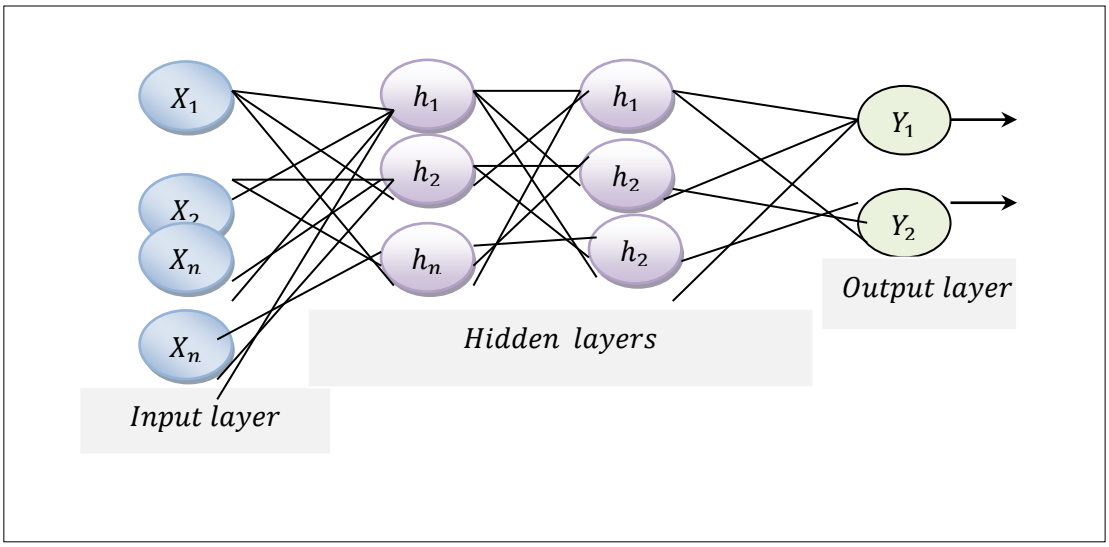

Figure 2 construction of deep structure multilayer neural network

The provided Figure 2 depicts the architecture of the deep structure multilayer neural network. The input layer accepts patient data, denoted $pd_1, pd_2, pd_3, \ldots . pd_m$ and associates it with a set of weights '$\varphi_1, \varphi_1, \ldots, \varphi_m$'. These weights are then combined with a bias term, k. Thus, the linear operation of the data and weight matrix may be expressed as follows:

$$X(t) = \sum_{i=1}^{m} pd_i * \varphi_i + \delta \quad (1)$$

The activity of the neuron at the input layer '$X(t)$' is calculated by multiplying the patient data 'pd_i' with the weights 'φ_i' and adding the bias 'δ', which has a stored value of '1'. The input is sent to the concealed layer where the process of data categorization takes place. Next, the patient data that has been gathered is examined in hidden layer 1 using the Tikhonov Regularised function. The process of identifying the correlation between one or more independent variables is used to determine the dependent variable, often known as the classes.

Tikhonov regularisation using a general form Regularisation aims to improve the accuracy of output identification by minimising the discrepancy between testing and training data.

$$W = \arg\min \frac{1}{n} [\|pd_T - pd_r\|^2] + \lambda\ \omega^2 \quad (2)$$

W represents the result of regularisation, pd_T represents the actual testing data, and pd_r represents the training data. The symbol λ represents a regularisation parameter, ω^2 represents the squared values of the model

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

coefficients, $\|pd_T - pd_r\|^2$ represents a loss function, $\lambda\ \omega^2$ represents a regularised term, and n represents the number of patient data. The regularisation values are given to the activation function to get the classification outcomes. The suggested deep learning classifier utilises the tangent hyperbolic function to generate the output results.

The hyperbolic tangent function determines the result based on a certain group of inputs. The activation function is expressed mathematically as follows:

$$Y \to H = \frac{2}{1+\exp(-2W)} - 1 \quad (3)$$

In this context, H represents the tangent hyperbolic function, whereas W represents the results of regularisation. Y represents the output of a classifier. According to the outcomes of the activation function, the patient data have been accurately categorised. The activation function yields results within the range of '-1' to '+1'.

The error rate for each categorization result is calculated as follows: $R_e = \frac{1}{n}\left\|Y_o - Y_p\right\|^2$ (4)

Here, R_e reflects the rate of error, Y_o represents the actual classification results, and 'Y_p' signifies the output generated by the activation function. To minimise the error, the starting weight is adjusted using the stochastic gradient descent approach.

$$\varphi_{t+1} = \varphi_t * \eta \left[\frac{\partial R_e}{\partial \varphi_t}\right] \quad (5)$$

In this context, φ_{t+1} represents an updated weight, φ_t represents the current weight, and η specifies a learning rate $(\eta < 1)$. A higher learning rate enables the classifier to learn more quickly compared to a lower number. The expression '$\frac{\partial R_e}{\partial \varphi_t}$ represents the partial derivative of the error 'R_e' with regard to the current weight 'φ_t'. This technique is performed until the smallest error is found. Ultimately, the categorised outcomes are acquired at the output layer. The following is the algorithmic procedure for a stochastic gradient Tikhonov regularised deep multilayer neural network:

// Algorithm 1: stochastic gradient Tikhonov regularized deep multilayer neural network

Input: Dataset, patient data $pd_1, pd_2, pd_3, \ldots . pd_m$
Output: patient data classification

Begin
1. **Number of** patient data $pd_1, pd_2, pd_3, \ldots . pd_m$ taken **in the input layer**
2. **For each** patient data pd_i
3. Assign set of weight **'φ'** and add bias ' δ'
4. Measure the neuron activity at the input layer using (1)
5. **End For**
6. **For each training** patient data **–[hidden layer]**
7. **For each testing** patient data
8. Measure the correlation using (2)
9. **End For**
10. **End For**
11. Apply tangent hyperbolic function activation function
12. patient data is categorized into particular class
13. **End if**
14. **For each classification results**
15. Measure the error rate 'R_e'
16. Apply stochastic gradient descent
17. Update the initial weight 'φ_{t+1} '
18. Find minimum error
19. Obtain the final classification results with minimum error **at the output layer**
20. **End for**

End

Algorithm 1 outlines the various stages involved in classifying patient data. The proposed deep neural network classifier has many layers for the analysis of patient data. The patient data numbers are sent to the input layer. The

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

weights are assigned to each input in the set and then merged using the bias function. Afterwards, the input is sent to the hidden layer. The current phase is analysing the correlation between the testing and training data using generalised Tikhonov regularisation. Afterwards, the regularisation outcome is sent to the activation function in the hidden layer. The activation function assesses the regularisation outcome and produces the classified results. Afterwards, the error rate is determined by comparing the actual results of classification with the observed outcomes. In order to minimise the error, the initial weight is modified by the use of the stochastic gradient descent process. This process is repeated until the algorithm reaches the minimum degree of error. Ultimately, the classification results are obtained at the output layer.

3.2 Linear Congruential Generative Goldwasser–Micali Cryptosystem based secure data transmission

Following the data classification, the Goldwasser-Micali Cryptosystem is employed for secure data transmission. Public-key cryptography, a cryptographic technology, employs a pair of correlated keys - a public key and a private key - to encode and decode patient data, protecting it from unauthorised entry. The proposed cryptographic method provides heightened data transmission security by successfully reducing potential risks.

The Goldwasser-Micali scheme has three primary procedures: key generation, encryption method, and a deterministic decryption technique.

During this procedure, a unique set of cryptographic keys, consisting of a private key and a public key, is produced for every user. Let's examine two distinct prime numbers, R and S, both of which are enormous $R \neq S$.

$$U = R * S \quad (6)$$

$$V = G^2 \, mod \, U \quad (7)$$

Where 'G' represents a randomly produced value using the Lehmer random number generator. The Lehmer random number generator is a linear congruential generator specifically designed for producing prime numbers.

$$G = b.\ Z \ mod \, q \quad (8)$$

R is a randomly generated prime number, Z represents an initial value that is coprime to q, $mod\, q$ represents a prime modulus, and the multiplier b is an element with a high multiplicative order modulo q. Thus, the generation of the private and public key pair occurs in the following manner:

$$K_{pb} = (U, V) \quad (9)$$

$$K_{pr} = F\,(U, V) \quad (10)$$

In this context, K_{pb} represents a public key, K_{pr} represents a private key, and F represents a factorization. By following this process, the user's private and public keys are produced to ensure safe transfer of data.

Following the process of key creation, the server proceeds to distribute the keys to the users. Given the vulnerable and accessible setting, safeguarding patient data is of utmost importance. Thus, the user carries out data encryption using the key that was produced. Encryption is the transformation of original patient data into cypher text.

The user wants to convert the input data pd into a binary string.

$$pd \ \rightarrow B_1, B_{2,} B_3 \ldots B_b \quad (11)$$

The symbols $B_1, B_{2,} B_3 \ldots B_b$ represent individual bits of a string. The encrypted text is produced in the following manner:

$$CT = g^2 \, V^{B_i} \, (mod \, U) \quad (12)$$

The term CT represents a cypher text, g represents an integer value extracted from 'U', B_i represents the bit string of patient data, and V represents the public key of the receiver. After the encryption process is completed, the user transmits the cypher text to the server for storage.

When an authorised user wishes to retrieve patient data using the private key, which involves prime factorization denoted as $i.e\, F\,(U, V)$, the process of decryption is executed to acquire the original data. The original messages are derived for each cypher text using the following method.

$$B_i = Q(mod \, U) \quad (13)$$

The number Q is considered a quadratic residue of U (i.e. $mod\, U$), when $b_i$equals 0. Otherwise, b_i is equal to 1. Finally, the user obtains the original data. This technique enables the restriction of patient data access on the cloud server to just authorised users. This enhances the encryption and protection of data transmission between the client and server. The suggested algorithm is explained as follows:

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

// Algorithm 2: Linear Congruential Generative Goldwasser–Micali Cryptosystem based secure data transmission

Input : Number of users, classified patient data $pd_1, pd_2, pd_3, \ldots . pd_m$
Output: Improve data confidentiality

Begin
// **key generation**
Step 1: For each users
Step 2: Server generate pair of keys K_{pb} and K_{pr}
Step 3: End for
// **Encryption**
Step 4: For each patient data 'pd_i'
Step 5: Encode data into bit string using (11)
Step 6: Convert bit string into cipher text ' CT'
Step 7: User send cipher text 'CT' and store to server
Step 8: **End for**
// **Decryption**
Step 9 : for each cipher text
Step 10: Receiver decrypts data with private key (K_{pr})
Step 11: Obtain string 'B_i'
Step 12: Get original patient data 'pd '
Step 13: end for
End

Z procedure of securely transmitting data in the cloud using the Linear Congruential Generator is outlined in a systematic manner. Goldwasser–Micali Cryptosystem is presented for gaining improved data secrecy and integrity. At first, the cloud server creates a set of keys for each user to use for encrypting and decrypting data. Then the user executes data encryption and transferred to the server. The server gathers the unencrypted text and stores it. The recipient securely retrieves the data using their own cryptographic key, therefore preventing any unauthorised access. This method improves the secure transmission of data by increasing data secrecy.

4. Experimental setup

The SEMcrypt approach, in addition to the Robust and lightweight secure access strategy [1] and LABSE[2], were implemented in Java using the WUSTL EHMS 2020 Dataset for Internet of Medical Things (IoMT) Cybersecurity Research. The dataset was obtained from the website https://www.cse.wustl.edu/~jain/ehms/index.html. The numeral 21. The WUSTL-EHMS-2020 dataset was created using a real-time Enhanced Healthcare Monitoring System (EHMS). This dataset includes the aggregation of network traffic measurements and patients' biometrics. The patients' health data is collected from the sensors attached to their bodies and sent to the hospital server over the internet. An adversary intercepts the transfer of this patient data before it reaches the hospital server. Therefore, it is crucial to identify any unauthorised entry or attacks, such as man-in-the-middle attacks using spoofing and data injection, that could take place during the transmission of patient data in the cloud. The dataset consists of 16,000 instances, with each instance possessing 44 distinct features. The characteristics consist of 35 network flow measurements, eight patients' biometric attributes, and one output label, which may be either 0 or 1. The samples containing the assailant are labelled as 1, while the other samples are labelled as 0. Table 1 displays the biometric features of the eight patients.

Table 1 patient's biometric features

1	TEMP	Temperature in degrees Celsiusv
2	SPO_2	Blood oxygen
3	Pulse Rate	Pulse Rate in BPM (Beats Per Minute).
4	SYS	SYStolic blood pressure
5	DIA	DIAstolic blood pressure.
6	Heart Rate	Heart Rate in Beats Per Minute (BPM)
7	Resp_Rate	Respiration Rate in BPM

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

8	ST	Electrically neutral area between ventricular depolarization (QRS complex) and repolarization (T wave) in millivolts (mv).

5. Performance results analysis

This section presents a performance study of the proposed SEMcrypt approach and two other secure access schemes, namely Robust and lightweight secure access scheme [1] and LABSE [2]. The analysis considers many factors including key generation time, confidentiality rate, integrity rate, calculation time, and classification accuracy.

Key generation time: The key generation process encompasses the duration needed to produce a pair of keys, namely the public key and secret key, which are used for the purposes of encrypting and decrypting data.

$$KG_{time} = NPD * Time\left(K_{pb} + K_{pr}\right) \quad (14)$$

The key generation time, denoted as 'KG_{time}', is determined by the number of patient data points 'NPD', the time required to produce the public key 'K_{pb}', and the time required to generate the private key 'K_pr' in a certain session. The duration of key production is quantified in milliseconds (ms).

Table 2 Comparison of key generation time

Number of patient data	key generation time (ms)		
	SEMcrypt	Robust and lightweight secure access scheme	LABSE
1600	6.5	12.2	10.3
3200	8.3	14.2	12.7
4800	10.4	15.7	13.8
6400	11.22	17.12	14.52
8000	13.01	18.23	15.75
9600	14.32	19.3	16.1
11200	16.45	20.4	17.5
12800	18.23	21.3	19.6
14400	19.03	22.9	21.5
16000	20.1	24.1	23.2

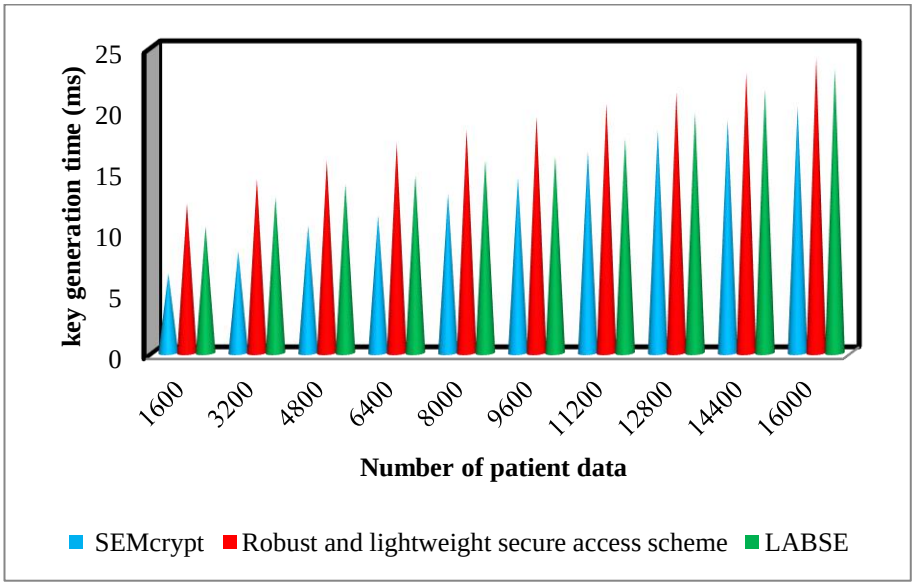

Figure 3 Graphical illustration of key generation time

Table 2 and figure 3 depict the key generation time performance for secure message transmission between users and a server in a cloud environment. The SEMcrypt approach and the Robust and lightweight secure access

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

strategy [1], LABSE [2] are used for this purpose. The quantity of data being transferred in this experiment varies between 1600 and 16000 for the purpose of experimentation. The key generation time on a cloud server is quantified in milliseconds (ms). According to figure 3, the time it takes to generate a key increases as the volume of transferred data increases. However, the time required for key production was significantly reduced when producing both the public and private keys. As an example, when the data count is 1600, the time taken to generate a key using the SEMcrypt approach was 6.5 milliseconds. Additionally, the time taken to generate the public key and secret key was found to be 12.2 milliseconds and 10.8 milliseconds respectively, as mentioned in references [1] and [2]. Simulations were done using varying amounts of data, and the resulting outcomes were compared. The comparative findings indicate that the key generation time of the SEMcrypt approach is decreased by 28% and 19% in comparison to [1] and [2] correspondingly. The reason for this is the use of the Lehmer random number generator in conjunction with the Goldwasser-Micali cryptography method. This combination allows for the efficient generation of prime numbers, which are then used to construct the key pairs required for encryption and decryption.

Data confidentiality rate: The metric is determined by calculating the proportion of patient data that is safeguarded against unauthorised access by potential attackers. The data secrecy rate is determined by mathematical calculation as follows:

$$CR = \left[\frac{PDP}{NPD}\right] * 100 \quad (15)$$

From (15), represents the level of secrecy. PDP refers to the quantity of patient data that is safeguarded, while NPD represents the quantity of patient data. Thus, the level of secrecy is quantified as a percentage (%).

Table 3 Comparison of confidentiality rate

Number of patient data	Confidentiality rate (%)		
	SEMcrypt	Robust and lightweight secure access scheme	LABSE
1600	95.75	89.06	91.87
3200	97.5	86.12	90.93
4800	98.33	87.81	89.79
6400	97.65	88.37	90.78
8000	98.12	86.2	88.75
9600	98.5	87.76	89.58
11200	98.66	88.35	91.18
12800	98.82	86.87	91.79
14400	97.22	88.54	90.62
16000	98.12	87.63	91.01

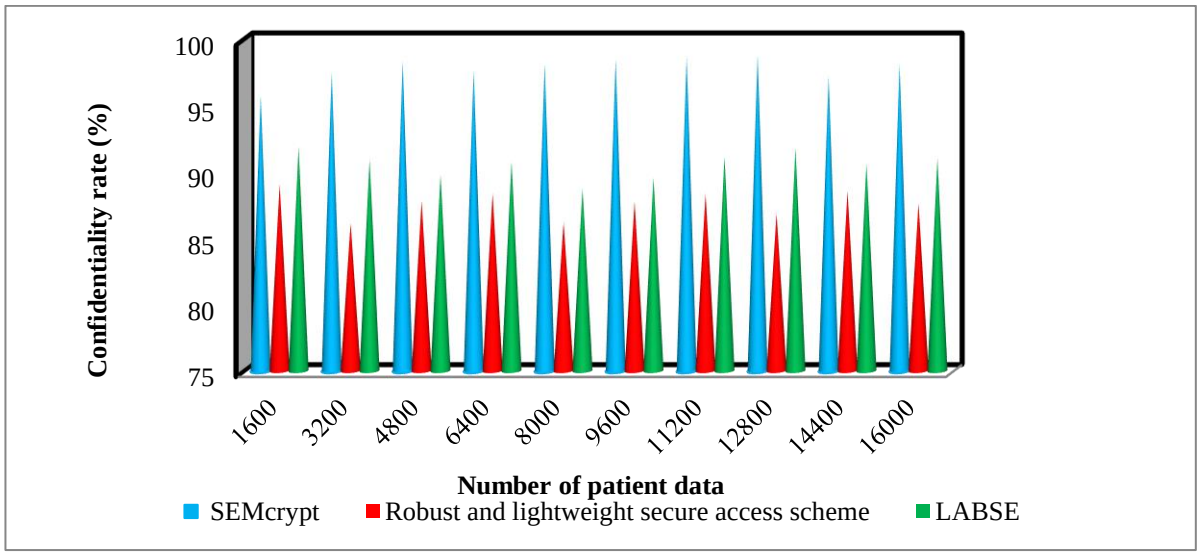

Figure 4 Graphical illustration of confidentiality rate

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

Figure 4 depicts a comparison of the confidentially rates of three algorithms: SEMcrypt method, Robust and lightweight secure access strategy [1], and LABSE [2]. The y-axis reflects the level of confidentially, while the x-axis shows the number of tasks. The following figure clearly demonstrates that the suggested SEMcrypt outperforms patient data with a confidentiality rate of 1600. Specifically, the confidentially rate values for SEMcrypt approach [1] and [2] are 95.75%, 89.06%, and 91.87%, respectively. Similarly, varying performance outcomes are found for each approach in relation to the quantity of patient data. Ultimately, the SEMcrypt approach is evaluated in relation to the current findings. The average comparison findings show that the data confidentially rate has increased by 12% and 8% when utilising the SEMcrypt methodology approach compared to [1] and [2], respectively. The primary factor behind this enhancement was the use of Linear Congruential Generative Goldwasser-Micali encryption and decryption for secure data transport. The patient data is first encrypted using the recipient's public key, resulting in the creation of cypher text. The data sent to the server is encrypted. The designated recipient decrypts the encrypted message using their authorised and valid private key. This method serves to prevent unauthorised users, namely attackers, from gaining access to the data. Consequently, this enhances the degree of data secrecy.

Data integrity rate: The term refers to the proportion of patient data that remains unaltered or unmodified by unauthorised individuals, such as attackers. The process of ensuring data integrity may be summarised as follows:

$$IR = \left[\frac{PDNM}{NPD}\right] * 100 \quad (16)$$

IR represents the Integrity Rate, PDNM represents patient data that has not been edited by an authorised user, and NPD represents the quantity of patient data. The integrity rate is quantified as a percentage (%).

Table 4 Comparison of Integrity Rate

Number of patient data	Integrity Rate (%)		
	SEMcrypt	Robust and lightweight secure access scheme	LABSE
1600	94.06	86.87	88.75
3200	96.87	84.37	89.37
4800	97.91	86.45	88.85
6400	96.87	87.5	89.37
8000	97.5	85.25	87.5
9600	97.08	86.71	88.54
11200	97.76	87.10	90.62
12800	97.26	86.32	90.82
14400	96.87	87.84	90.27
16000	97.81	86.87	90.75

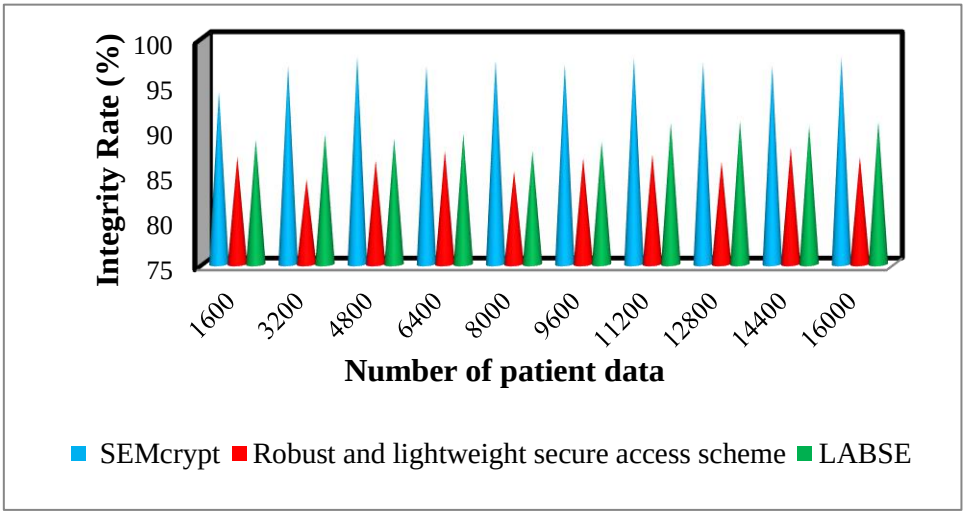

Figure 5 Graphical illustration of integrity rate

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

Figure 5 illustrates the performance outcomes of the integrity rate while using the SEMcrypt approach, as well as the Robust and lightweight secure access system [1] and LABSE [2]. Figure 4 displays a representation of 16,000 patient data points on the x-axis as part of the experimental procedure. The y-axis represents the integrity rate. For each approach, 10 iterations are conducted in this simulation to assess the integrity rate of data transfer. Based on the above graph, it can be seen that the SEMcrypt approach results in a superior data integrity rate. For the first iteration of the experiment, we will analyse a dataset consisting of 1600 data points. The SEMcrypt approach had an observed integrity rate of 94.06%. Furthermore, the integrity rate of the aforementioned [1] and [2] was determined to be 86.87% and 88.75% correspondingly. The aggregate performance of ten separate findings demonstrates a significant improvement of 12% in the integrity rate when utilising the SEMcrypt approach, compared to [1], and an 8% improvement compared to [2]. The improvement was attributed to the implementation of the Linear Congruential Generative Goldwasser-Micali encryption algorithm. The cryptographic technique under consideration uses the Linear Congruential generator to produce a set of keys for every data transfer. These keys are used for the execution of data encryption and decryption procedures. Hence, the data is accessed by the authorised user who has a valid key. Furthermore, the original data remained unaltered by the intruders or attackers, hence enhancing the data integrity rate.

Computation time: Algorithmic efficiency refers to the duration required for a secure transmission of patient data from the sender to the recipient. The total time consumption is mathematically computed as follows:

$$CT = N * t\,[STD] \quad (17)$$

CT symbolises the duration of a calculation, N represents the quantity of patient data, 't' symbolises time, and STD signifies the safe transmission of a single piece of data. Hence, the total processing time is quantified in milliseconds (ms).

Table 5 Comparison of computation time

Number of patient data	computation time (ms)		
	SEMcrypt	Robust and lightweight secure access scheme	LABSE
1600	19.2	25.6	22.4
3200	25.92	32	28.8
4800	31.2	36	33.6
6400	35.2	41.6	38.4
8000	42.4	48	44
9600	49.92	55.68	52.8
11200	51.52	58.24	56
12800	55.04	61.44	58.88
14400	56.16	64.8	60.48
16000	59.2	65.6	62.4

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

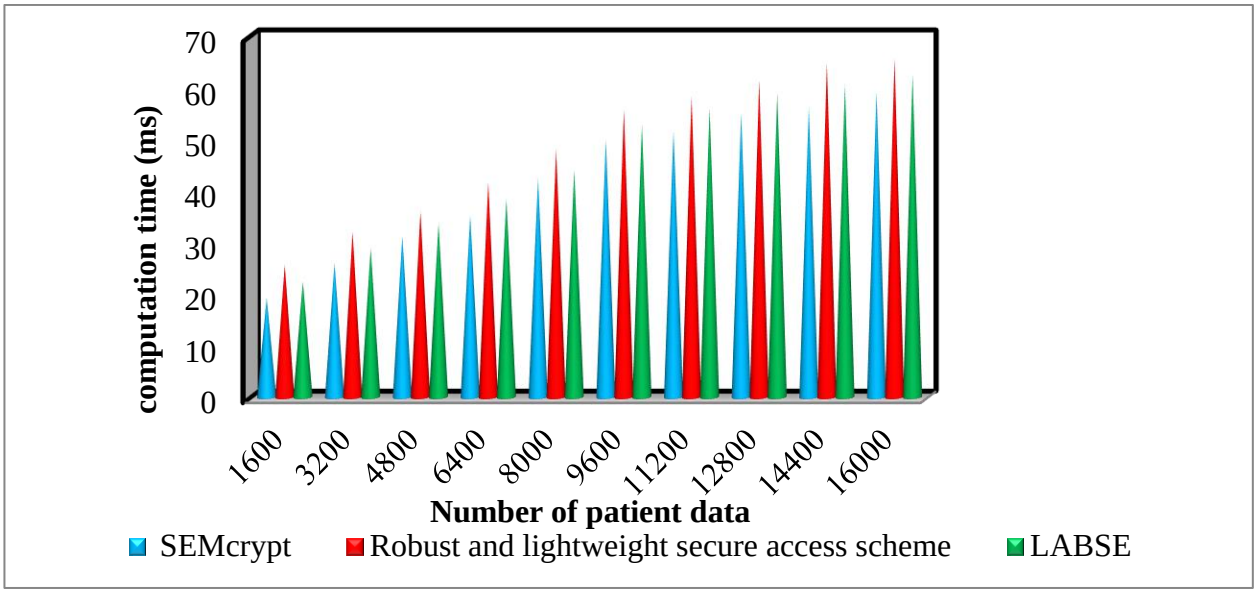

Figure 6 Graphical illustration of computation time

Figure 6 depicts the comparison of calculation time between three methods: SEMcrypt approach, Robust and lightweight secure access system [1], and LABSE [2]. The graph illustrates the relationship between calculation time (y-axis) and the number of patient data (x-axis), which spans from 1600 to 16000. The preceding chart clearly demonstrates that the proposed SEMcrypt methodology outperforms previous techniques [1] and [2] in terms of performance. As the quantity of patient data increases, the computational time also increases. According to the figure above, when there are 1600 patient data, the calculation time for the SEMcrypt method, as well as techniques [1] and [2], is 19.2ms, 25.6ms, and 22.4ms respectively. The SEMcrypt approach reduces the total calculation time for secure data transfer from user to server by 14% and 8% compared to [1] and [2], respectively. This is due to the use of a stochastic gradient regularised deep multilayer neural network for the purpose of categorising patient data into distinct groups. The deep multilayer neural network employs generalised Tikhonov regularisation to analyse patient data and classify using the hyperbolic tangent function. Following the categorization, the suggested cryptographic strategy is used to provide safe data transfer while minimising computation time.

Classification accuracy: The accuracy is determined by calculating the ratio of properly categorised patient data to the total amount of data used for assessment. The calculation of categorization accuracy is as follows:

$$Acc_{cl} = \left[\frac{PDCC}{NPD}\right] * 100 \quad (18)$$

In this context, the term Acc_{cl} represents the accuracy of data classification. '$PDCC$' refers to the number of patient data that have been successfully categorised, while 'NPD' represents the total quantity of patient data. The classification accuracy is quantified as a percentage (%).

Table 6 Comparison of Classification accuracy

Number of patient data	Classification accuracy (%)		
	SEMcrypt	Robust and lightweight secure access scheme	LABSE
1600	96.87	90.62	93.75
3200	98.43	87.5	92.03
4800	98.95	89.58	90.62
6400	98.43	89.06	92.18
8000	98.87	87.12	89.37
9600	98.43	88.54	90.62
11200	99.10	89.28	91.96
12800	99.21	87.5	92.57

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

14400	98.61	88.88	91.66
16000	98.75	88.12	91.25

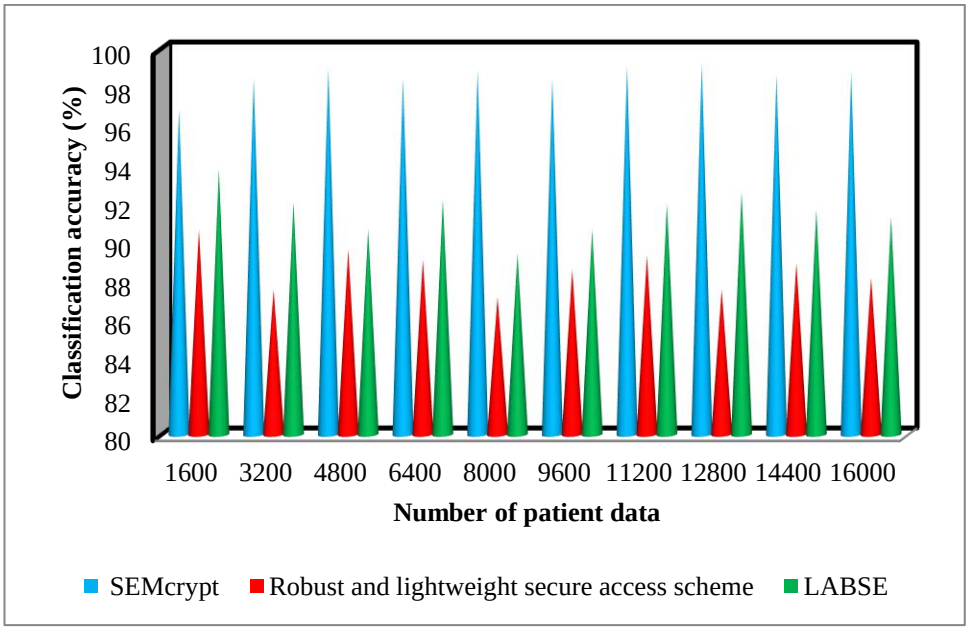

Figure 7 Graphical illustration of Classification accuracy

The performance analysis of classification accuracy with respect to number of patient data is illustrated in figure 7. Also, with the experiment is conducted using 1600 patient data and actually 1550 data being 96.8% using SEMcrypt technique and 90.62% and 93.75% of classification accuracy were observed by using Robust and lightweight secure access scheme [1] and LABSE [2]. With this result, the overall classification accuracy was found to be better using SEMcrypt technique than [1] and [2]. The overall performance of classification accuracy using SEMcrypt technique was considerably improved by 11% and 8% compared to [1] and [2] respectively. This is due to the application of stochastic gradient regularized deep multilayer neural network to classify the patient data into different classes. The deep neural network uses the generalized Tikhonov regularization and tangent function for data classification. Finally, gradient descent function is applied to minimize the error and improves the classification accuracy.

6. Conclusion

This work presents the development of a new cryptographic algorithm called SEMcrypt, which addresses security concerns in cloud-assisted healthcare systems. The advent of cutting-edge technology in cloud computing has brought about a heightened concern for security, which is now the foremost challenge in this field. This framework implements the encryption and decryption procedure by using the Linear Congruential Generative Goldwasser–Micali cryptographic approach. Initially, a stochastic gradient regularised deep multilayer neural network is used for the purpose of data classification. Subsequently, the categorised data is encrypted using the Linear Congruential Generative Goldwasser-Micali cryptographic algorithm, ensuring safe data transfer while minimising computational time. Consequently, the SEMcrypt approach enhances the security of data transmission between users and servers, leading to increased levels of data confidentiality and integrity. Various simulations were conducted using multiple criteria, including key generation time, secrecy rate, integrity rate, calculation time, and classification accuracy. The performance results demonstrated that the SEMcrypt methodology had superior performance compared to the current techniques.

References

[1] Mehedi Masud, Gurjot Singh Gaba, Karanjeet Choudhary, Roobaea Alroobaea & M. Shamim Hossain, "A robust and lightweight secure access scheme for cloud-based E-healthcare services", Peer-to-Peer Networking and Applications, Springer, 2021, Pages 1-15. https://doi.org/10.1007/s12083-021-01162-x

[2] Yangyang Bao, Weidong Qiu, Xiaochun Cheng, "Secure and Lightweight Fine-Grained Searchable Data Sharing for IoT-Oriented and Cloud-Assisted Smart Healthcare System", IEEE Internet of Things Journal, Volume 9, Issue 4, 2022, Pages 2513 – 2526. **DOI:** 10.1109/JIOT.2021.3063846

[3] Sherief H. Murad, Kamel H. Rahouma, "Implementation and Performance Analysis of Hybrid Cryptographic Schemes

applied in Cloud Computing Environment", Procedia Computer Science, Elsevier, Volume 194, 2021, Pages 165-172. https://doi.org/10.1016/j.procs.2021.10.070

[4] L. Selvam and J. Arokia Renjit, "On developing dynamic and efficient cryptosystem for safeguarding healthcare data in public clouds", Journal of Ambient Intelligence and Humanized Computing, Springer, Volume 12, 2021, Pages 3353–3361. https://doi.org/10.1007/s12652-020-02033-8

[5] Fursan Thabit, Sharaf Alhomdy, Sudhir Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing", Global Transitions Proceedings, Elsevier, Volume 2, Issue 1, 2021, Pages 100-110. https://doi.org/10.1016/j.gltp.2021.01.014

[6] Sheng Peng ,Zhiming Cai ,Wenjian Liu, Wennan Wang, Guang Li, Yutin Sun, and Linkai Zhu, "Blockchain Data Secure Transmission Method Based on Homomorphic Encryption", Computational Intelligence and Neuroscience, Hindawi, Volume 2022, April 2022, Pages 1-9. https://doi.org/10.1155/2022/3406228

[7] Jusak Jusak, Seedahmed S. Mahmoud, Roy Laurens, Musleh Alsulami, Qiang Fang, "A New Approach for Secure Cloud-Based Electronic Health Record and its Experimental Testbed", IEEE Access, Volume 10, 2021, Pages 1082 – 1095. **DOI:** 10.1109/ACCESS.2021.3138135

[8] Aneruth Mohanasundaram and, Aruna S.K, "Improved Henon Chaotic Map-based Progressive Block-based visual cryptography strategy for securing sensitive data in a cloud EHR system", International Journal of Intelligent Networks, Elsevier, Volume 3, 2022, Pages 109-112. https://doi.org/10.1016/j.ijin.2022.08.004

[9] S Sasikumar, K Sundar, C Jayakumar, Mohammad S. Obaidat , Thompson Stephan, Kuei-Fang Hsiao, "Modeling and simulation o f a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment", Simulation Modelling Practice and Theory, Elsevier, Volume 121, 2022 , Pages 1-11. https://doi.org/10.1016/j.simpat.2022.102651

[10] Remya Sivan and Zuriati Ahmad Zukarnain, "Security and Privacy in Cloud-Based E-Health System", Symmetry, Volume 13, Issue 5, 2021, Pages 1-14. https://doi.org/10.3390/sym13050742

[11] Ding Li, Wang Zhongsheng, Wang Xiaodong, Wu Dong, "Security information transmission algorithms for IoT based on cloud computing", Computer Communications, Elsevier, Volume 155, 2020, Pages 32-39. https://doi.org/10.1016/j.comcom.2020.03.010

[12] Ala Saleh Alluhaidan, "Secure Medical Data Model Using Integrated Transformed Paillier and KLEIN Algorithm Encryption Technique with Elephant Herd Optimization for Healthcare Applications", Journal of Healthcare Engineering, Hindawi, Volume 2022, October 2022, Pages 1-14. https://doi.org/10.1155/2022/3991295

[13] Sandeep kaur ,Gaganpreet kaur , and Mohammad Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing", Security and Communication Networks, Hindawi, Volume 2022, March 2022, Pages 1-9. https://doi.org/10.1155/2022/7540891

[14] Dheresh Soni, Deepak Srivastava , Ashutosh Bhatt , Ambika Aggarwal , Sunil Kumar , and Mohd Asif Shah, "An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol" , Mathematical Problems in Engineering, Hindawi, Volume 2022, 1 September 2022, Pages 1-14. https://doi.org/10.1155/2022/4696649

[15] Munwar Ali, Low Tang Jung, Ali Hassan Sodhro, Asif Ali Laghari, Samir Birahim Belhaouari, Zeeshan Gillani, "A Confidentiality-based data Classification-as-aService (C2aaS) for cloud security", Alexandria Engineering Journal, Elsevier, Volume 64, 1 2023, Pages 749-760. https://doi.org/10.1016/j.aej.2022.10.056

[16] Arvind Panwar ,Vishal Bhatnagar ,Manju Khari ,Ahmad Waleed Salehi , and Gaurav Gupta, "A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake", Computational Intelligence and Neuroscience, Hindawi, Volume 2022, April 2022, Pages 1-19. https://doi.org/10.1155/2022/3045107

[17] Feras M. Awaysheh , Mohammad N. Aladwan, Mamoun Alazab ,Sadi Alawadi, José C. Cabaleiro , and Tomá, "Security by Design for Big Data Frameworks Over Cloud Computing", IEEE Transactions on Engineering Management , Volume 69, Issue 6, 2022, Pages 3676 – 3693. **DOI:** 10.1109/TEM.2020.3045661

[18] Maryam Shabbir, Ayesha Shabbir, Celestine Iwendi ,Abdul Rehman Javed, Muhammad Rizwan, Norbert Herencsar, And Jerry Chun-Wei Lin, "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing", IEEE Access, Volume 9, Pages 8820 – 8834. **DOI:** 10.1109/ACCESS.2021.3049564

[19] Jiguo Li, Hao Yan, and Yichen Zhang, "Efficient Identity-Based Provable Multi-Copy Data Possession in Multi-Cloud Storage", IEEE Transactions on Cloud Computing , Volume 10, Issue 1, 2022, Pages 356 – 365. **DOI:** 10.1109/TCC.2019.2929045

[20] Shimao Yao, Ralph Voltaire J. Dayot, Hyung-Jin Kim,In-Ho Ra , "A Novel Revocable and Identity-Based Conditional Proxy Re-Encryption Scheme With Ciphertext Evolution for Secure Cloud Data Sharing", IEEE Access, Volume 9, Pages 42801 – 42816. **DOI:** 10.1109/ACCESS.2021.3064863

[21] Anar A. Hady, Ali Ghubaish, Tara Salman, Devrim Unal, Raj Jain , "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study", IEEE Access , Volume 8, 2020, Pages 106576 – 106584. **DOI:** 10.1109/ACCESS.2020.3000421