Journal of Theoretical and Applied Information Technology
30th April 2026. Vol.104. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

LINEAR MULTIPLICATIVE CRYPTOSYSTEM BASED DEEP NEURAL LEARNING CLASSIFIER MODEL FOR DATA TRANSACTION SECURITY IN CLOUD COMPUTING

SHAKIRA P V [1], LAXMI RAJA [2]

[1]Research Scholar, Department of CSE, Faculty of Engineering, Karpagam Academy of Higher Education Coimbatore – 641021.
[2]Assistant Professor, Department of Cyber Security, Faculty of Engineering , Karpagam Academy of Higher Education
Coimbatore – 641021.
Email: [1]shakirapv@myyahoo.com [2]journals856@gmail.com

ABSTRACT

Cloud computing has emerged as a significant platform due to its rapid condition of computing resources for data analysis. Cloud data are stored and accessed on remote servers, allowing users to access them from anywhere at any time. As number of CU increases, there is a growing need to protect the data of various users. Security is main concern because information is broadcasted to remote servers more than channel. Previous to data transactions occur at cloud computing, safety demands required to mentioned. Therefore, a novel Linear Multiplicative Cryptosystem-based Deep Neural Learning Classifier (LMC-DNLC) model has been developed to facilitate secure data transactions from cloud users to cloud servers with enhanced data confidentiality and reduced time consumption. The LMC-DNLC model encompasses four processes namely key generation, encryption, classification, and decryption. Each user registers their details and generates session key pairs using the Joye-Libert Cryptosystem with the assistance of a Linear Multiplicative generator. Subsequently, user data is encrypted using Joye-Libert encryption and transmitted to CS. On server side, the classification of authentic or illegitimate users is performed by DNLC. The Forbes similarity coefficient is applied to deep learning for analyzing user keys, classifying genuine users with the help of a soft-step activation function. Finally, genuine users are decrypted using Joye-Libert decryption to attain original information. This process ensures secure data transactions with higher data confidentiality between users and cloud servers. Experimental assessment is conducted on various factors concerning number of CU and data. Outcomes of quantitative analysis indicate that the LMC-DNLC model provides an efficient solution for attaining superior data confidentiality and integrity, reducing communication, computation overhead compared to existing methods.

Keywords: *Cloud, Security In Data Transaction, Deep Neural Learning Classifier, Joye-Libert Cryptosystem, Linear Multiplicative Generator, Forbes Similarity Coefficient, Soft-Step Activation Function,*

1.INTRODUCTION

CC is computing model employed for saving, processing, accessing information. With the rapid expansion of cloud services, a large amount of data is shared through cloud computing, enabling diverse users to share data under specific access control policies. The dynamic and distributed nature of cloud environments presents unique challenges at defending sensitive data as of unauthorized access, and so on during data transmission. Many cryptographic methods have designed to enhance big data security in CC.

A data storing and sharing system named Smart Crypt was developed in [1]. This system provides users with the capability to securely distribute their encrypted data and ensuring data confidentiality through the implementation of symmetric homomorphic encryption. But it inefficient for high-volume and high-velocity cloud data sharing system. A Hybrid Elliptic Curve Cryptography (HECC) method was introduced in [2] with the objective of enhancing cloud data security. This method inimizes computational and communication overhead but it did not improve the performance of data integrity A method for safe information group sharing as well as conditional distribution through minimal computation time was

designed in [3]. However, ML method was not used to improve result of secure information sharing with minimum overhead. A cloud-backed storage scheme was introduced in [4] to efficiently save and distributes big data to protect the sensitive personal information. However, the computational overhead was not reduced.

A secure and collusion-resistant proxy re-encryption protocol was introduced in [5] for group data sharing. The model successfully reduces computation costs but achieving efficient data integrity posed a significant challenge. A blockchain-based encryption method was developed in [6] with the aim of ensuring secure data sharing. The method enhances data confidentiality, but the overhead associated with secure data sharing remained unaddressed. An effective lightweight homomorphic cryptographic algorithm was designed in [7] to improve the safety of information sharing. A Secure Authentication as well as Data Sharing method was introduced in [8]. But it failed to accelerate encryption as well as decryption operations for cloud data sharing.

The Proficient Security over dispersed Storage technique, introduced [9], aimed to achieve secure data transmission with reduced computational time. But, result analysis of data confidentiality was not addressed. Blockchain-assisted method was designed [10] for safe and reliable information sharing. However, it failed to detect a malicious data owner who presents undesirable data to disrupt the system.

- To enhance safety of information sharing in cloud, LMC-DNLC model is developed.
- Firstly, Joye-Libert cryptography is utilized to generate the session key for each cloud user with the help of a linear multiplicative generator.
- The Joye-Libert encryption is performed to upload multiple pieces of information on CS, minimizing communication overhead.
- LMC-DNLC model utilizes a Deep Neural Learning Classifier to identify authentic or illegitimate users based on the Forbes similarity coefficient.
- Finally, extensive experiments are performed to estimate result of LMC-DNLC model as well as other conventional works.

In Section 2, literature review in area of cloud computing are explained. Section 3 provides complete description of LMC-DNLC model, outlining its various processes. Sections 4 cover experimental analysis and database explanation followed by a comparative analysis of different methods. lastly, Section 5 provides conclusion of work.

2.LITERATURE REVIEW

An efficient as well as empirical cloud framework for secure data communication using the fuzzy c-means (FCM) algorithm was introduced in [11]. However, the computational efficiency was not improved as it did not incorporate machine learning and novel cryptographic techniques. An enhanced RSA-based role-basis access control method was designed [12] to ensure comprehensive protection of sensitive information.

An efficient and secure model was developed in [13] for facilitating data sharing. The model utilizes asymmetric pairing and features compact size ciphertext, aiming to enhance the speed of the learning process. But the overhead involved in data sharing was not reduced. An access control method based on blockchain was introduced in [14] for cloud computing to ensure security and minimize both computation and communication overhead.

A multi-cloud platform was developed in [15 to enhance the privacy and high availability of data. A secure communication system was developed [16] using an ensemble Voting Classifier and Elliptic Curve Cryptography to minimize computation costs during online data sharing in a multi-cloud environment. However, the method did not achieve higher integrity.

A new Decentralized Blockchain-based Security (Deblock-Sec) model was introduced in [17] for resource-constrained environments, aiming to address security concerns through the implementation of lightweight cryptographic algorithms. However, the procedure was found to be inefficient in identifying legitimate users, to improve overall efficiency. A Blockchain-based collaborative data sharing method was designed [18]. However, data confidentiality was not enhanced by the Blockchain-based scheme. A secure computation using the (k, n) threshold secret-sharing technique was introduced [19] through minimal communication overhead. Policy-based Broadcast Access Authorization (PBAA) method was developed in [20] by introducing key-policy attribute-based encryption.

3. PROPOSAL METHODOLOGY

Journal of Theoretical and Applied Information Technology
30th April 2026. Vol.104. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Cloud is a computing paradigm that provide as services over the Internet. In scenario where the big volume of data resides within the cloud, the authorized users access the data. During the data access, there exists a chance for unauthorized users enters and alters information in cloud. So, a new technique is required to verify confidentiality, authenticity, integrity of data transmission in the cloud. In this paper, a novel LMC-DNLC model is introduced for safe data broadcast and also guarantees data confidentiality as well as integrity.

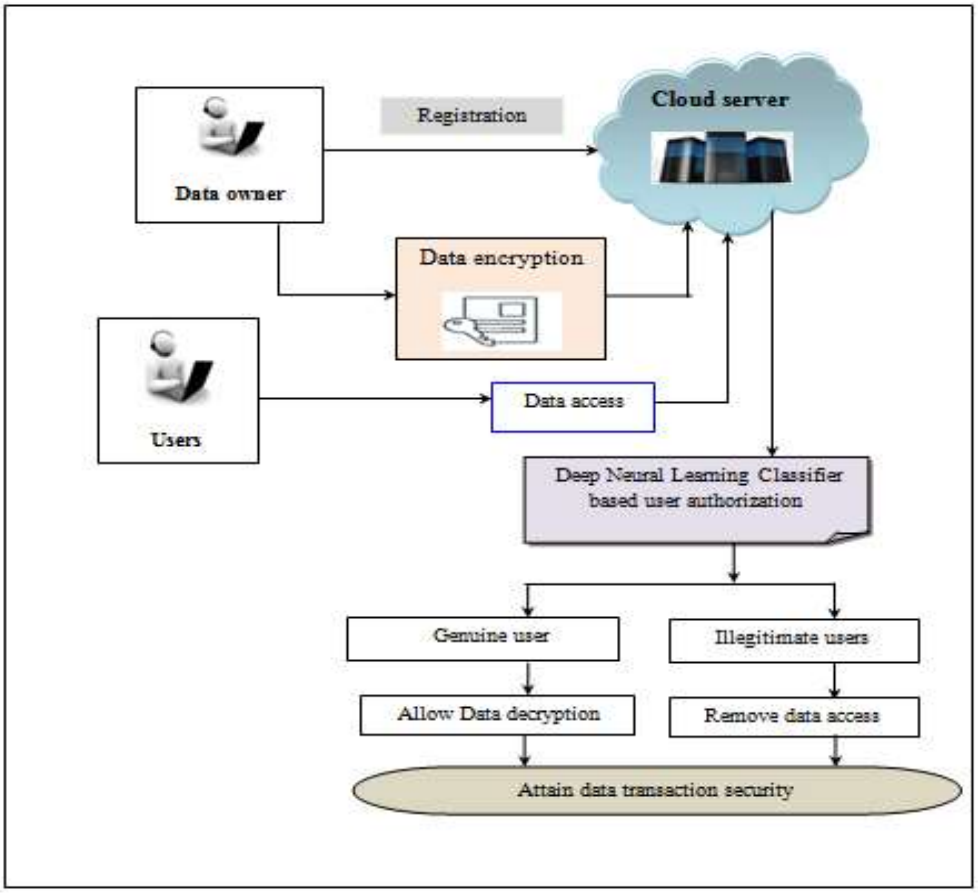

Figure 1 structural design of the proposed LMC-DNLC method

Figure 1 illustrates process of LMC-DNLC model for safe data communication among CU as well as cloud server. Cloud architecture comprises three entities: the cloud server cloud users 'CS' and cloud users $U_1, U_2, U_3, \ldots U_n$, data owners contributing to secured data access. Initially, cloud users and data owners perform the registration process to store their data for subsequent processing. Following this, CS creates pair of keys for every registered user. Subsequently, data owners perform data encryption, and the encrypted information is uploading on CS. While a user intends to entrance information from server, the server performs verification to distinguish genuine or illegitimate users using the Deep Neural Learning Classifier. The server grants the data access to genuine users and removed access for illegitimate users. Genuine users access the data through performing the decryption to ensure data integrity and confidentiality.

3.1 Key generation

In framework of CC, the registration and key generation processes act fundamental task in

establishing secure communication between cloud users as well as the cloud server. The registration process establishes user identity and access controls, while the key generation process enables secure communication for encrypting and decrypting user data.

In the registration process, user provides necessary information, such as user identification, personal details, and possibly other authentication factors. The registration process is essential for the CSP to create as well as manage user accounts securely.

Key generation is a fundamental part of secure communication in the cloud. CS creates pair of cryptographic keys for every registered user. This key pair consists of a public key , private key. Public key is communal as private key is reserved secret. This pairing key is employed for data encryption as well as decryption. .

Proposed technique utilizes the Joye–Libert cryptosystem, which is considered a generalization of Goldwasser–Micali public key cryptography. The significant advantage of the Joye–Libert scheme over Goldwasser–Micali is its support for a larger message space. Consequently, it considerably reduces the expansion of the ciphertext.

In the key generation process, Lehmer generators is used for generating the two large prime numbers r and s such that $r \neq s$. A Lehmer generator is a linear multiplicative random number generator.

$$r = (a.x_n) \bmod Q \quad (1)$$

$$s = (b.x_n) \bmod Q \quad (2)$$

Where, r,s denotes random number generated, x_i represents current value in sequence , a,b are multipliers. The parameters 'a', 'b' and Q are carefully chosen to ensure good properties of the generated number. Therefore, the Lehmer generators are used for generating pseudorandom numbers in a specific range.

Therefore, the session private key ' K_r' is generated as given below,

$$K_r = (r,s) \quad (3)$$

The session publicly key 'K_b' is generated as given below,

$$K_b = (X,R,G) \quad (4)$$

Where, R denotes a random number, G denotes an integer ($G>1$).

$$X = r * s \quad (5)$$

From (3) (4), a session public key as well as private key are generated for every user.

3.2 Public key encryption

After key generation process, data owner sends their data to server in the form of cipher text. The cipher text is obtained though the encryption process. Encryption is the process of transforming the data to unreadable form. Result of the encryption is ciphertext. Major aim of encryption is to secure confidentiality of user information, guarantying which authorized user entrance as well as appreciate data. By applying Joye–Libert cryptosystem, the encryption is performed with public key of the user.

First, input data is separated to number of message bits. Let's consider the input data as 'D', and the division into message bits is mathematically represented as follows,

$$\mathrm{D} = B_1, B_2, B_3 .. \; B_k \quad (6)$$

After the division process, for each plain text ($0 < B < 2^k$) the encryption is performed with session public key as follows,

$$T = G^B . R^{2^k} \bmod X \quad (7)$$

Where, T indicates a cipher text, G denotes a random element, B indicates message bit, R, represents public key, $X=r*s$, 2^k indicates a power residue symbol. After the encryption, the ciphertext is generated and it sends to cloud server for data storage to guarantee the data confidentiality.

3.3 Deep Neural Learning Classifier based user authorization

When user entrances saved information, server identifies authentic or illegitimate users using

Deep Neural Learning Classifier for accessing the data or removing the access. Deep Neural Learning Classifier is an artificial feed forward NN that includes many layers for processing provided input.

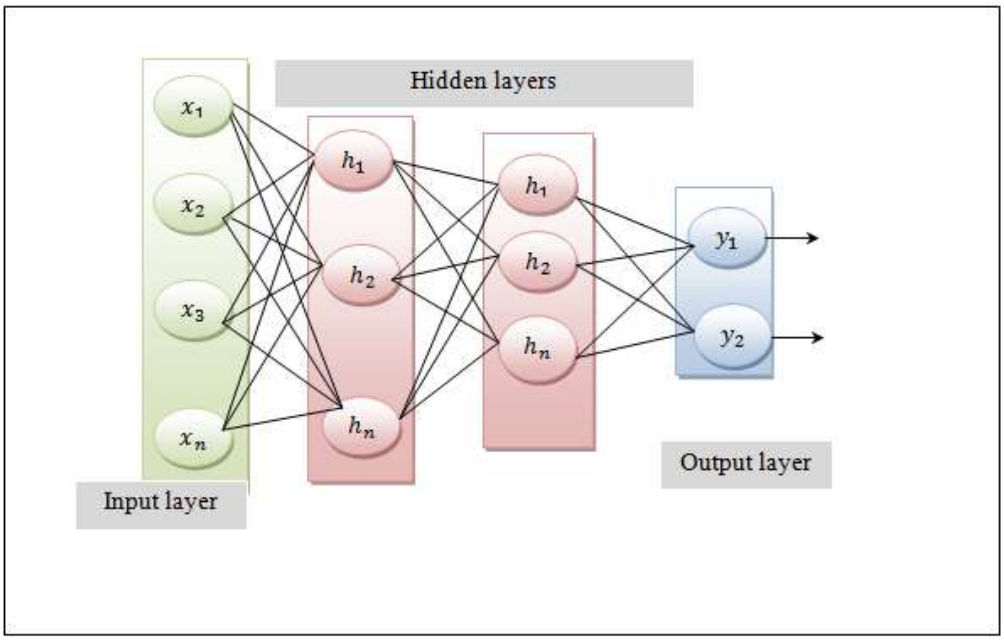

Figure 2 structural designs of Deep Neural Learning Classifier

Figure 2 depicts structure of DNLC of feed-forward artificial neural network for classification of cloud users with a multiple layer of nodes. It contains four layers, such as one input layer, two hidden layers as well as one output layer.

Input Layer(*x*): This layer receives input.

Hidden Layers (*h*): layer among input as well as output layers are called hidden layers. It contains nodes (or neurons) that process the input through weighted connections.

Output Layer (*y*): The final layer produces the overall processed output

Each layer includes a small individual unit called node or neuron. Neurons in every layer are associated to neurons in subsequently layer, every connection has weight. Connections among neurons are connected through weights that are regulated through training procedure.

Initially, number of cloud users is collected at an input layer.

$$U = \{U_1, U_2, U_3, \ldots . U_n\} \quad (8)$$

Where, U denotes a 'n' number of cloud users. The activity of a neuron in each layer computes a linear function of the weighted sum of its inputs, summed by the bias term.

$$A = \sum_{i=1}^{n} U_i \ \beta_i + w \quad (9)$$

Where, A denotes an activity of neuron, U_i denotes a 'n' number of users, β_i synaptic weight, 'w' indicates a bias term that has the integer value of '1'.

The input of the 'n' number of cloud users are transferred into the hidden layer. With the input users, server performs the user verification through the Forbes similarity coefficient. It is a similarity measure between two sets namely user login keys and previously saved key at time of registration. It is defined as the product of the size of the intersection of the sets and the total number of elements in the vectors, divided by the product of the sizes of the sets. Mathematically, the Forbes similarity coefficient is formulated as given below,

$$FC = N * \frac{|L(K) \cap S(K)|}{|L(K)||S(K)|} \quad (10)$$

Where, FC denotes a Forbes similarity coefficient, N indicates a total number of elements in the set (the length of the vectors), $L(K)$ denotes a user login keys, $S(K)$ stored keys at the time of registration, $|L(K) \cap S(K)|$ denotes a mutual dependence between the two sets, $|L(K)|$ denotes a size of the sets '$L(K)$', $|S(K)|$ indicates a size of the sets '$S(K)$'. The Forbes similarity gives output value between 0 and 1. It reaches its maximum value of '1' when the sets are matching, meaning all elements in both sets are the same. Otherwise, the similarity provides output value of 0.

Similarity coefficient values are provided to soft-step activation function to analyze results as well as provide classification results as authentic or illegitimate users.

$$F = \frac{1}{(1+\exp(-FC)} \quad (11)$$

Where, F denotes a soft-step activation function, FC deenotes a Forbes similarity coefficient. The output of the sigmoid function falls between 0 and 1.

$$F = \begin{cases} 1\,; & authentic \\ 0\,; & illegitimate\ users \end{cases} \quad (12)$$

If the output value reaches 1, the user is classified as authentic; otherwise, they are classified as illegitimate users. The classification results are obtained at the output layer.

3.4 Decryption

Once the authentic and illegitimate users are identified, CS allows entrance only to authentic users as well as removes access for illegitimate users. This helps enhance data integrity. The authentic users decrypt cipher text and obtain innovative information. Decryption is performed using Joye–Libert cryptosystem, with private key of the authentic user.

For each cipher text, the original data gets obtained through the decryption with private key as follows,

$$D = T^s \bmod X \quad (13)$$

Where, the value D be a original data, T denotes a cipher text, s denotes a private key This process helps to only certified user is allowed to communicate the data from cloud server and remove the access for other users. This helps to improve security of data communication between the cloud users and server.

Algorithm 1: Linear Multiplicative Cryptosystem-based Deep Neural Learning Classifier

Input: dataset D, number of cloud users $U_1, U_2, U_3, \ldots U_n$, data $D_1, D_2, D_3, \ldots D_m$, cloud server '$CS$', Data owner

Output : Increase security of data transaction

Begin

Registration

Step 1: **Collect** number of cloud users $U_1, U_2, U_3, \ldots U_n$
Step 2: **For** each user 'U_i'
Step 3: Perform registration process
Step 4: CS' generate the pair of session key using (3) (4)
Step 5: **End for**
Step 6:

Encryption

Step 7: **For** each user data 'D_i'
Step 8: Divide number of message blocks D = $B_1, B_2, B_3 \ldots B_k$
Step 9: Perform encryption with public key using (7)
Step 10: Send encrypted data into server
Step 11: **End for**

Classification

Step 12: **For each access request**
Step 13: Server performs the user authorization
Step 14: **Collect the number of users in input layer**
Step 15: **for each user**
Step 16: **for each user** login keys
Step 17: Measure the similarity using (10)
Step 18: **End for**
Step 19: **End for**
Step 20: Apply activation function using (11)
Step 21: **If** ($F = 1$) **then**
Step 22: User classified as authentic
Step 23: **else**
Step 24: User classified as illegitimate
Step 25: **End if**

Decryption

Step 26: Authentic user decrypt the data using (13)
Step 27: Obtain the original data
End

Algorithm 1, as described above, outlines the steps involved in securing data transactions between a cloud server and users. Procedure starts through server generating a session key pair for each registered user to help secure communication. Subsequently, cloud users transform their data into an encrypted format, enhancing confidentiality, and transmit it to CS to avert unauthorized access. When a user tries to entrance information, CS initiates a classification process with DNLC. The classifier takes number of cloud users as input in input layer. The Forbes similarity coefficient is then employed to measure the similarity between the user login keys for data access and the stored keys. The soft step activation function is applied to classify users as either authentic or illegitimate based on the results of the Forbes similarity coefficient. The outcomes of this classification process are obtained at the output layer. Finally, authenticated users perform decryption to retrieve original data as of CS. This approach ensures the security and privacy of data during transmission and access within the cloud environment.

4. EXPERIMENTAL ANALYSIS

Experimental assessment of LMC-DNLC model and existing [1] [2] are executed using by as well as cloudsim simulator for safe data communication at CC. To perform execution, Amazon access sample database collected as of https://archive.ics.uci.edu/ml/datasets/Amazon+Access+Samples. Dataset is characterized by sparse information including user profiles and their

associated access permissions. The file incorporates four distinct categories of attributes. In this dataset, a binary labeling system is employed: users are assigned the label '1' if they have added access to a particular data, and '0' indicates a remove access'

4.1 Performance metrics description

Performance of LMC-DNLC model as well as conventional SmartCrypt [1], HECC [2] is measured through dissimilar metrics.

Data confidentiality rate: It is measure of number of information accessed through a genuine user as well as deprived of access for an illegitimate user in cloud. It is expressed as below

$$Rate_{DC} = \left[\frac{Number\ of\ data\ protected}{m}\right],$$

Where, $Rate_{DC}$ represent the data confidentiality rate, m indicates number of data that calculated in percentage (%).

Table 1 comparison of $Rate_{DC}$

Number of data	$Rate_{DC}$ (%)		
	LMC-DNLC	SmartCrypt	HECC
10000	97.52	90.52	92.55
20000	96.83	89.27	91.11
30000	97.88	88.50	90.51
40000	98.805	89.15	92.13
50000	98.25	88.85	90.51
60000	97.75	89.44	90.42
70000	96.52	89.22	92.21
80000	97.48	88.20	90.70
90000	98.36	87.29	91.74
100000	98.12	88.96	90.65

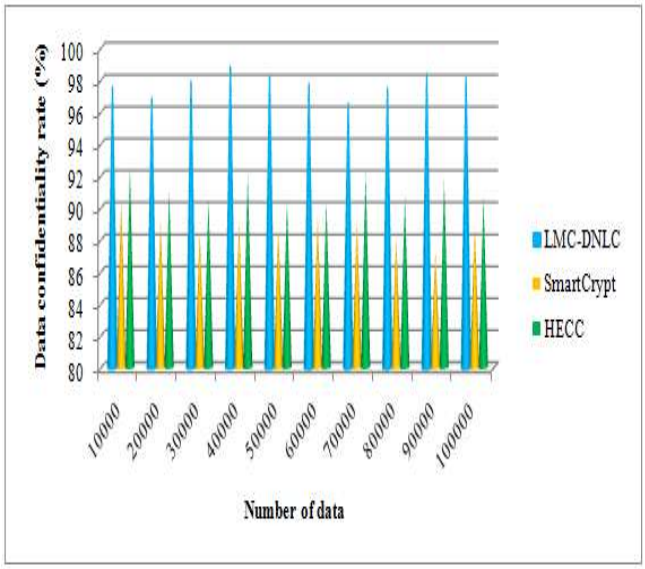

Figure 3 performance outcomes of $Rate_{DC}$

Figure 3 depicts result outcomes of $Rate_{DC}$ using proposed LMC-DNLC model and the existing Smart Crypt [1] and HECC [2]. Results demonstrate that the proposed LMC-DNLC model outperforms, achieving superior $Rate_{DC}$compared to [1] and [2]. Specifically, in an experiment with 10,000 data, the confidentiality rate using the proposed LMC-DNLC model was observed to be 97.52%, whereas the existing methods [1] and [2] achieved confidentiality rates of 90.52% and 92.55%, respectively. The overall performance across ten results reveals a significant increase in the confidentiality rate using the proposed LMC-DNLC model, with a 10% improvement compared to [1] and a 7% improvement compared to [2]. This improvement is achieved through the use of the Joye-Libert cryptosystem in the LMC-DNLC model, which encrypts the data before uploading it to the cloud, thereby enhancing data confidentiality. Additionally, the Deep Neural Learning Classifier categorizes users as genuine or illegitimate based on the similarity coefficient. The server grants access to genuine users while removing access to others, further enhancing confidentiality in data transactions among user as well as CS.

Data integrity rate: It is calculated as count of information which remains unaltered or unchanged through some illegitimate users. It is expressed as below:

Where, $Rate_{DI}$ indicates data integrity rate, m represents number of data that is calculated in percentage (%).

$$Rate_{DI} = \left[\frac{Number\ of\ data\ not\ altered}{m}\right] * 100 \quad (15)$$

Table 2 comparison of $Rate_{DI}$

Number of data	$Rate_{DI}$ (%)		
	LMC-DNLC	SmartCrypt	HECC
10000	96.98	89.55	92
20000	96.2	89	90.52
30000	96.85	88.16	89.51
40000	97.75	88.5	91.25
50000	97.04	88.6	89.71
60000	96.84	88.75	90.08
70000	95.09	87.93	91.85
80000	96.57	87.75	89.44
90000	97.55	86.65	90.05
100000	97.12	87.25	89.85

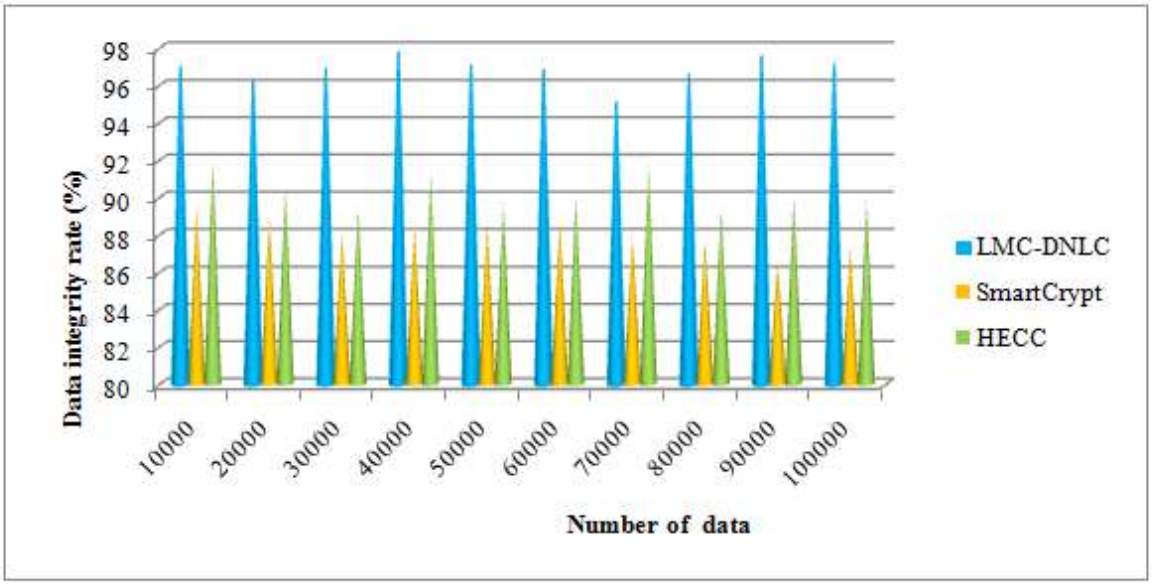

Figure 4 performance outcomes of data integrity rate

Figure 4 depicts result investigation of $Rate_{DI}$ by three different techniques. In Figure 4, $Rate_{DI}$ was found to be higher using the LMC-DNLC model compared to the existing methods. However, in experiments performed through 10,000 data, $Rate_{DI}$ was observed 96.98% with LMC-DNLC model, and it was 89.55% and 92% using methods [1] and [2], respectively. This improvement is achieved through the application of the Joye-Libert cryptosystem for session key pair generation with the assistance of a linear multiplicative generator. These keys act vital part in encrypting and decrypting information. Consequently, unauthorized users were unable to alter or modify any data, enhancing data integrity during communication between the cloud user and server.

Communication overhead: The evaluation involves determining the amount of memory required for sharing secure data. Mathematically, this is formulated as follows:

$$CMO = \sum_{i=1}^{m} D_i * Mem[SD] \quad (16)$$

Where, the communication overhead '*CMO*' is calculated depend on number of data 'D_i' and memory utilized in performing data sharing '*Mem[SD]*' respectively. It is calculated in megabytes (MB).

Table 3 comparison of *CMO*

Number of data	*CMO* (MB)		
	LMC-DNLC	SmartCrypt	HECC
10000	30	38	35
20000	40	52	46
30000	54	60	57
40000	60	72	68
50000	70	80	75
60000	78	90	84
70000	84	98	91
80000	92	104	96
90000	108	126	117
100000	110	130	120

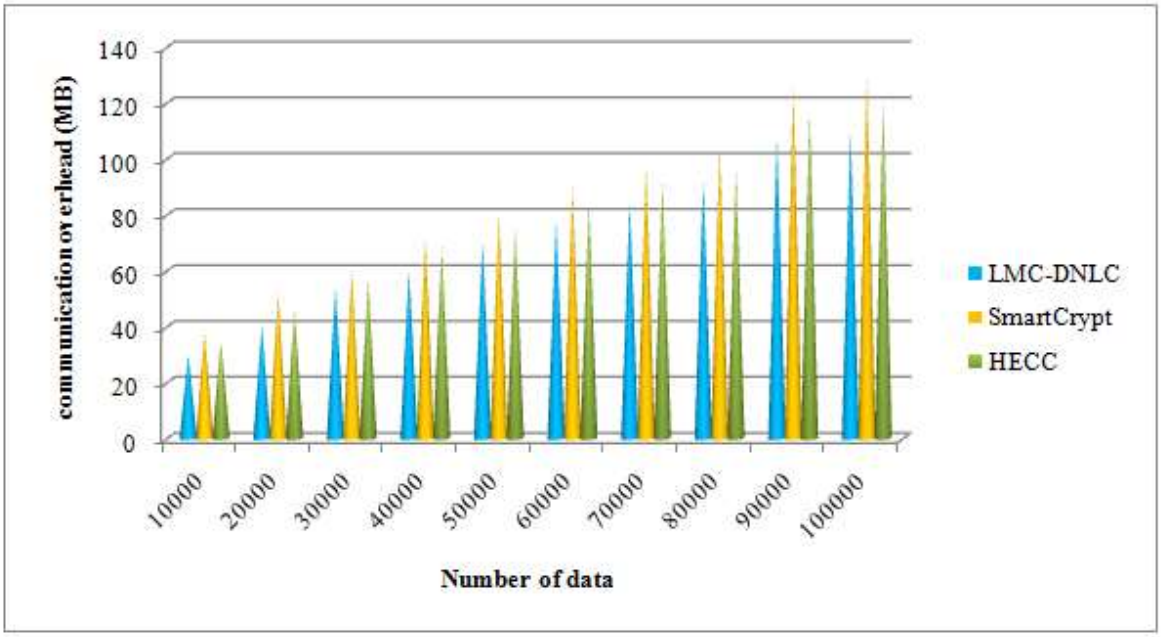

Figure 5 performance outcomes of *CMO*

Figure 5 depicts performance outcomes of *CMO* in secure data transmission. In Figure 5, *CMO* of LMC-DNLC model is reduced compared to existing methods. Additionally, as number of input data enhances, *CMO* of all three methods also increases. The experiment was conducted with 10,000 data in initial iteration. Result of *CMO* with LMC-DNLC model was 30MB, whereas *CMO* was 38MB , 35MB by [1] and [2], respectively. Similarly, various results of *CMO* were examined. Observed outcomes of LMC-DNLC model are compared to existing techniques. Entire comparison outcomes show which *CMO* involved at secure information sharing with LMC-DNLC model is reduced by 15% , 9% than the [1] and [2], respectively. This reduction is attributed to the Joye-Libert cryptosystem performing data encryption to obtain the ciphertext, which is then uploaded to the cloud server. This procedure reduces overhead of data communication among CS as well as the user.

Computation overhead: It is calculated as amount of time taken for secure data sharing between cloud user and server.

$$CO = \sum_{i=1}^{m} D_i * t\,(SD) \qquad (17)$$

Where, CO indicates a computation overhead, D_i data, $t\,(SD)$ represents time for sharing the single data. It is calculated in milliseconds (ms).

Performance outcomes related to computation overhead are depicted in Figure 6. Graphical representation clearly demonstrates that the computation overhead of the LMC-DNLC model is lower than that of the other two methods [1] [2]. For instance, when considering a 10,000 data, the time consumption for secure data sharing using the LMC-DNLC model was found to be 45ms, and the time consumption for [1] and [2] were 55ms and 50ms. Different performance results were observed for each method with varying numbers of information. Entire comparison outcomes of LMC-DNLC model were compared to outcomes of conventional methods.

Through this performance analysis, it was determined that the computation overhead using the LMC-DNLC model decreased by 17% compared to [1] and 9% compared to [2]. This reduction is achieved by the application of the Joye-Libert Cryptosystem with the Deep Neural Learning Classifier, which enhances secure data encryption. The Deep Neural Learning Classifier accurately identifies authorized or unauthorized users before access, resulting in shorter time consumption for safe data sharing at cloud.

Table 4 comparison of CO

Number of data	CO (ms)		
	LMC-DNLC	SmartCrypt	HECC
10000	45	55	50
20000	50	60	54
30000	57	69	63
40000	64	80	70
50000	70	82.5	75
60000	78	90	81
70000	84	98	92.4
80000	89.6	112.8	104
90000	108	127.8	121.5
100000	113	135	126

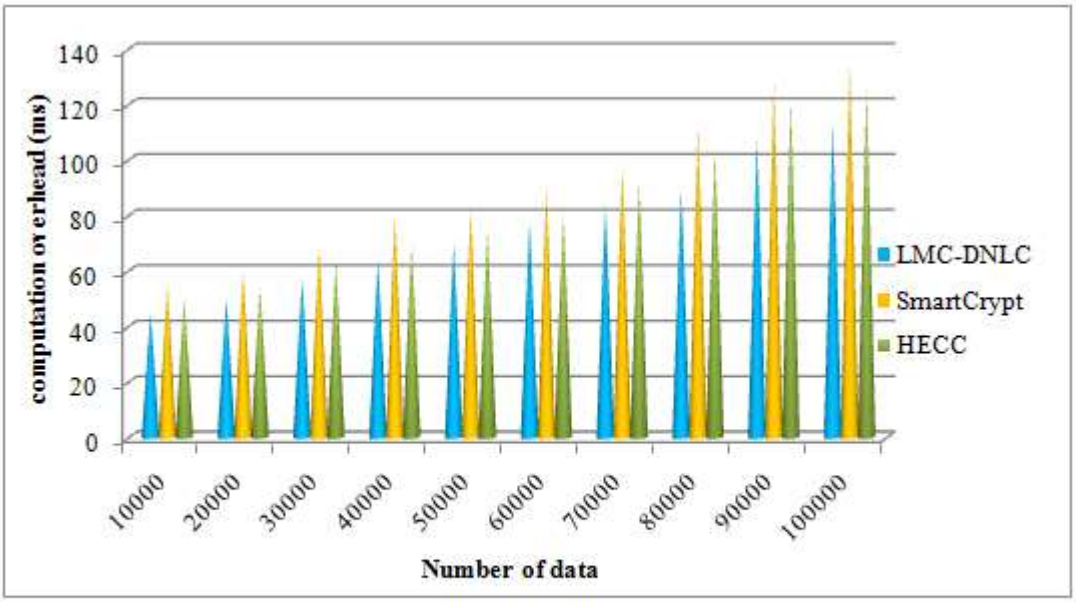

Figure 6 performance outcomes of computation overhead

5. CONCLUSION

Data security and privacy are major concerns for users in cloud computing to protect the data confidentiality. In this paper, an efficient and secure LMC-DNLC model is developed to facilitate secure sharing of a large amount of data, aiming to reduce memory consumption in a cloud computing environment. The data owner encrypts the data

before uploading it to the cloud server using Joye-Libert encryption. The proposed cryptosystem efficiently generates session keys to ensure the security of shared data and prevent malicious user involvement during data sharing. Additionally, the Deep Neural Learning Classifier accurately identifies malicious users and genuine users in the cloud, providing access control. A comprehensive experimental assessment is conducted by considering varying amounts of data, and the results of proposed model are compared through two existing algorithms. Observed numerical results confirm that the proposed LMC-DNLC model achieving a higher confidentiality rate, integrity rate, and minimizing communication and computation overhead compared to other existing methods.

REFERENCES

[1]Subir Halder and, Thomas Newe, "Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT", Future Generation Computer Systems, Elsevier, Volume 133, August 2022, Pages 351-363. https://doi.org/10.1016/j.future.2022.03.032

[2] B. Ranganatha Rao and , B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security", Measurement: Sensors, Elsevier, Volume 29, 2023, Pages 1-12. https://doi.org/10.1016/j.measen.2023.100870

[3] Qinlong Huang, Yixian Yang, Wei Yue and Yue He, "Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing", IEEE Transactions on Cloud Computing, Volume 9, Issue 4, 2021, Pages 1607-1618. **DOI:** 10.1109/TCC.2019.2908163

[4] Ricardo Mendes, Tiago Oliveira, Vinicius Cogo, Nuno Neves, and Alysson Bessani, "CHARON: A Secure Cloud-of-Clouds System for Storing and Sharing Big Data", IEEE Transactions on Cloud Computing, Volume 9, Issue 4, October-December 2021, Pages 1349 – 1361. **DOI:** 10.1109/TCC.2019.2916856

[5] Jian Shen, Huijie Yang, Pandi Vijayakumar, and Neeraj Kummar, "A Privacy-Preserving and Untraceable Group Data Sharing Scheme in Cloud Computing", IEEE Transactions on Dependable and Secure Computing, Volume 19, Issue 4, 2022, Pages 2198 – 2210. **DOI:** 10.1109/TDSC.2021.3050517

[6] Nabeil Eltayieb, Rashad Elhabob, Alzubair Hassan, Fagen Li, "A Blockchain-Based Attribute-Based Signcryption Scheme to Secure Data Sharing in the Cloud", Journal of Systems Architecture, Elsevier, Volume 102, January 2020, Pages 1-30. https://doi.org/10.1016/j.sysarc.2019.101653

[7] Fursan Thabit , Ozgu Can, Sharaf Alhomdy, Ghaleb H. Al-Gaphari, Sudhir Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing", International Journal of Intelligent Networks, Elsevier, Volume 3, 2022, Pages 16-30. https://doi.org/10.1016/j.ijin.2022.04.001

[8] Uma Narayanan, Varghese Paul, Shelbi Joseph, "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment", Journal of King Saud University - Computer and Information Sciences, Elsevier, Volume 34, Issue 6, 2022, Pages 3121-3135. https://doi.org/10.1016/j.jksuci.2020.05.005

[9] Fizza Shahid, Humaira Ashraf, Anwar Ghani, Shahbaz Ahmed Khan Ghayyur, Shahaboddin Shamshirband, And Ely Salwana, "PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud", IEEE Access , Volume 8, 2020, Pages 118285 – 118298. **DOI:** 10.1109/ACCESS.2020.3004433

[10] Yu Guo, Shenling Wang & Jianhui Huang, "A blockchain-assisted framework for secure and reliable data sharing in distributed systems", EURASIP Journal on Wireless Communications and Networking, Springer, Volume 2021, Pages 1-19. https://doi.org/10.1186/s13638-021-02041-y

[11] 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, September 2022, Pages 1-14. https://doi.org/10.1155/2022/4696649

[12] A. Kousalya and Nam-kyun Baik, Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique", International Journal of Intelligent Networks, Elsevier, Volume 4, 2023, Pages 62-67. https://doi.org/10.1016/j.ijin.2023.03.003

[13] Snehlata Yadav and Namita Tiwari, "An Efficient and Secure Data Sharing Method Using Asymmetric Pairing with Shorter Ciphertext to Enable Rapid Learning in Healthcare", Computational Intelligence and Neuroscience, Hindawi, Volume 2022, April 2022, Pages 1-13. https://doi.org/10.1155/2022/4788031

[14] Tonglai Liu, Jigang Wu, Jiaxing Li, Jingyi Li, Yidong Li, "Efficient decentralized access control for secure data sharing in cloud computing", Concurrency and Computation Practice and experience, Wiley, Volume 35, Issue 17, 2021, Pages 1-14. https://doi.org/10.1002/cpe.6383

[15] Yulliwas Ameur, Samia Bouzefrane, Le Vinh Thinh, "Handling security issues by using homomorphic encryption in multi-cloud environment", Procedia Computer Science, Elsevier, Volume 220, 2023, Pages 390-397. https://doi.org/10.1016/j.procs.2023.03.050

[16] Ashutosh Kumar Singh and Deepika Saxena, "A Cryptography and Machine Learning Based Authentication for Secure Data-Sharing in Federated Cloud Services Environment", Journal Of Applied Security Research, Volume 17, Issue 3, 2022, Pages 1-28. https://doi.org/10.1080/19361610.2020.1870404

[17] Uma Narayanan, Varghese Paul & Shelbi Joseph, "Decentralized blockchain based authentication for secure data sharing in Cloud-IoT", Journal of Ambient Intelligence and Humanized Computing, Springer, Volume 13, 2022, Pages 769 -787. https://doi.org/10.1007/s12652-021-02929-z

[18] Meng Shen, Junxian Duan, Liehuang Zhu, Jie Zhang, Xiaojiang Du, and Mohsen Guizani, "Blockchain-based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds", IEEE Journal on Selected Areas in Communications, Volume 38, Issue 6, 2020, Pages 1229 – 1241. **DOI:** 10.1109/JSAC.2020.2986619

[19] Keiichi Iwamura and Ahmad Akmal Aminuddin Mohd Kamal, "Communication-Efficient Secure Computation of Encrypted Inputs Using (k, n) Threshold Secret Sharing", IEEE Access Volume 11, 2023, Pages 51166 – 51184. **DOI:** 10.1109/ACCESS.2023.3278995

[20] Hua Deng, Jixin Zhang, Zheng Qin, Qianhong Wu, Hui Yin, Aniello Castiglione, "Policy-based Broadcast Access Authorization for Flexible Data Sharing in Clouds", IEEE Transactions on Dependable and Secure Computing, Volume 19, Issue 5, 2022, Pages 3024 – 3037. **DOI:** 10.1109/TDSC.2021.3080282