SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 11711-11720
Open Access. Online & Print

DOI: 10.5281/zenodo.124261110

A SECURE ENCRYPTION FRAMEWORK FOR OPTIMIZED DATA STORAGE AND RETRIEVAL IN CLOUD COMPUTING ENVIRONMENTS USING A BOUNDARY-INTEGRATED NEURAL NETWORK APPROACH

Sreeju P Sreedharan[1]*, M. Nithya[2], Sanjith Narayanan[3]

[1,2,3]CAIDS, Vinayaka Mission's Research Foundation, Salem, India.
Email: [1]sreeju@gmail.com, [2]nithya.ph.d@gmail.com, [3]sanjithnarayanan@hotmail.com

Received: 11/10/2025
Accepted: 18/02/2026

Corresponding Author: Sreeju P Sreedharan (sreeju@gmail.com)

ABSTRACT

As more distributed system technologies continue to rise, among the most urgent issues confronting the digital universe is securing sensitive and confidential information while in transit and storage, which is also most significant challenges cloud computing is facing. Several approaches to data security in storage of cloud computing. The most important approach to data protection is encryption. Consequently, a number of available encryption methods are utilized to ensure security, integrity, legitimate access using advanced cryptographic algorithms. Cloud computing is a new paradigm that has been widely embraced as platform for storing, analyzing user information. The cloud is accessed through internet, making data vulnerable to external, internal attacks. Cloud Service Providers now need to have secure architecture in place to identify cloud intrusions, protect customers' data from attackers, hackers. It integrates Boundary-Integrated Neural Network (BINN) and Twofish Encryption Algorithm (TEA) to identify and block unauthorized cloud access. The three stages of the system proposed are user registration, intrusion detection, intrusion prevention. The BINN classifier forecasts unauthorized access attempts by analyzing data access patterns, while TEA ensures secure encryption and authentication during both data storage and retrieval. During retrieval, only verified users can decrypt and access the data, thereby preserving confidentiality and preventing unauthorized access. The experimental results improved data security used to secure cloud computing applications. The performance of SEF-CCE-BINN algorithm showed good protection levels and significant security enhancement as well as increased execution rate compared to many algorithms that have been widely implemented in cloud computing.

INDEX TERMS: Boundary-Integrated Neural Network, Twofish Encryption Algorithm, Implicit Unscented Particle Filter, Starfish Optimization Algorithm.

I. INTRODUCTION

Many services are instantaneously available and reasonably priced because to new computer architecture called cloud computing [1]. The primary goal of cloud computing is to provide fast, easy data, compute storage for data [2]. Cloud computing and other modern computer architectures offer many instantaneously available attributes [3]. The primary idea behind cloud computing is to present specific functionalities for processing data in cloud-based systems [4]. The computing sector is well-suited to manage the risks and threats that CCE incurs [5]. Cryptography, essential element of cloud security, is one method of improving cloud computing security [6]. Additionally, it is a method for encrypting user's letter into cipher text, coded message that only designated receiver understand, reveal hidden message [7]. When data are being transmitted, confidentiality is preserved [8]. Cryptology is the mathematical process of controlling data integrity and authentication, such as encryption. Offering these security services is made feasible by the variety of reliable solutions that cryptography offers [9]. Digital signatures, encryption protocols, hashing approaches of many well-known encryption approaches are used to encrypt and decrypt private data marked by cryptography (Symmetric Methods, Hybrid Algorithms, Asymmetric Algorithms) [10].

With exponential growth of distributed system technologies and widespread use of cloud computing, security of sensitive, confidential data during transmission, storage has emerged as a significant challenge. Cloud platforms, although providing scalable and elastic data management solutions, bring user information under the risk of potential threats from both insider and external attacks by virtue of their web-based access model. Conventional security practices are usually not effective in detecting and countering sophisticated cloud intrusion attempts. Thus, there is a pressing need for strong security mechanisms that not only detect illegal access but also prevent possible breaches in advance. Inspired by the need to improve cloud security, this study introduces a collaborative framework using the Boundary-Integrated Neural Network (BINN) and Twofish Encryption Algorithm (TEA) for efficiently detecting and preventing unapproved cloud access, maintaining data integrity, confidentiality, and authorized access while outperforming conventional classifiers as regards security improvement and operational efficiency.

The system proposed incorporates a new fusion of the Boundary-Integrated Neural Network (BINN) and the Twofish Encryption Algorithm (TEA) to ensure cloud security through efficient intrusion prevention and detection. As opposed to conventional encryption-based or independent intrusion detection systems, the BINN classifier not only classifies legitimate vs. unauthorized access with high accuracy but also actively cooperates with TEA to validate user legitimacy during the data access process. This two-layer technique dramatically enhances the power of catching unusual access patterns and shutting down intruders in real-time. The experimental results show that this combined technique provides higher levels of security protection, faster execution, and overall better effectiveness analyzed to current methods. Through integration of sophisticated machine learning model with an optimization algorithm specifically designed for cloud environments, this research offers a new and more robust solution to long-standing problem of cloud data security.

Main contribution of research is given as below:

- The work proposes a new system combining the Boundary-Integrated Neural Network (BINN) with the Twofish Encryption Algorithm (TEA) for effective intrusion detection and avoidance of unauthorized access in cloud computing environments.
- A new process of three-phase user registration, intrusion detection, intrusion prevention is established to advance security of sensitive cloud information from both inside and outside intrusions.
- The BINN classifier is utilized to precisely predict cloud data access habits, detecting and blocking unusual or unauthorized access attempts with higher detection accuracy than standard techniques.
- The TEA is applied in the data access phase to check dynamically the validity of users, making the access control process more secure and ensuring only valid users have access to cloud resources.
- Comprehensive experiments confirm that the suggested SEF-CCE-BINN system substantially enhances security levels, execution time, and intrusion detection efficiency when compared with current cloud security algorithms.

The remainder of the manuscript is arranged as: Part 2 reviews literature; Part 3 outlines proposed method; Part 4 proves results and discussion; and Part 5 conclusion.

II. LITERATURE SURVEY

Numerous researches concerning SEF for Optimized Data Storage and Retrieval in CCE

utilizing DL, some of the current research works are reviewed here.

In 2023, Kanagala, P. and Jayaraman, R., [11] have suggested Stochastic Gradient Descent LSTM dependent secure encryption approach for cloud data storage and retrieval in CCE. Here, ensuring security of sensitive with private data through storage, transportation was most urgent issues facing the digital world due to the growing prevalence of distributed system technology. This was thought to be most significant challenges facing cloud computing. There are several ways to improve data security in storage environment of cloud computing. It attains higher specificity, low F1-score.

In 2024, Ahmad, S., et al., [12] have presented ML-dependent intelligent security syatem for secure cloud key management. Here, strong cryptographic key management is essential to guaranteeing availability, confidentiality, integrity of sensitive data in cloud environments. Ensuring security with dependability of critical management services is turning into crucial component of overall cloud security as cloud usage and data volumes grow. It provides low accuracy and high specificity.

In 2024, Akbar, M., et al., [13] have presented Enhanced authentication for de-duplication of big data on cloud storage system utilizing ML method. Here, An enormous amount of information that has been copied from several sources is called enormous information. It might be challenging to separate copied information from vast amounts of information. It suggests secure deduplication strategy for large-scale data storage. Cloud service providers enable customers to store, transfer data in effective and efficient manner. Cloud service providers enable customers to store, transfer data in effective and efficient manner. It attains higher F1-score, higher computational time.

In 2023, Wang, Y., et al., [14] have presented Efficient with secure content-dependent image retrieval with DNNs in MCC. To assist us document our lives and produce a lot of data in the process, smart devices provide a number of more practical forms. Many users outsource their image data directly to the cloud server because of the limitations of local storage. However, the cloud server's plaintext image storage is extremely unsafe, making it easy for image privacy information to leak. It provides low specificity and high accuracy.

In 2025, Ganesh, N.S.,et al, [15] have presented DL-dependent user authentication and hybrid encryption for secured blockchain-aided data storage with optimal task offloading in MEC. Here, MEC offers customers low-latency storage and effective compute services by integrating edge technologies. MEC is a quickly developing technique that provides cloud-based services at the network edge. MEC enables real-time, low-latency applications to run on Internet of Things (IoT) devices. Task offloading is vulnerable to security and privacy risks, too, including data tampering, data replication, leaks of private information. It provides high accuracy and low F1-score. Table 1 shows comparison table of literature survey.

TABLE I: Comparison Table of Literature Survey

Authors	Methods	Advantages	Disadvantages
Suganya & Sasipraba (2023)	Stochastic Gradient Descent (SGD) + LSTM for encryption in cloud	High security in cloud storage; adaptive encryption learning model	Computationally intensive; LSTM training may cause delays
Ahmad et al. (2024)	ML-based intelligent key management framework	Intelligent, automated key distribution; reduces human error	Potential vulnerability to adversarial ML attacks
Akbar et al. (2024)	ML-based enhanced authentication for de-duplication	Efficient storage through de-duplication; improved data validation	May face accuracy issues with similar yet distinct data; model drift risk
Wang et al. (2023)	DNN for CBIR	Accurate and secure image retrieval; suitable for mobile cloud	Model complexity; possible privacy concerns in CBIR
Ganesh et al. (2025)	Deep learning user authentication + hybrid encryption + blockchain in MEC	Multi-layered security; efficient task offloading; blockchain integrity	High system overhead; complexity in integration and deployment

The contrast between novel approaches to safe cloud computing showcases an assortment of ML and DL methods specifically adapted for various sides of data safety. One solution involves Stochastic Gradient Descent and LSTM networks combined to apply adaptive encryption for cloud data with powerful security at the expense of being highly computation-intensive. Another approach uses an intelligent machine learning-based system for cloud key management, enhancing automation and minimizing human error, but potentially vulnerable to adversarial attacks. Another technique uses machine learning for better authentication and data de-duplication in big data systems, maximizing storage efficiency but struggling with model accuracy over time. Deep neural networks are also used for secure and robust content-

dependent image retrieval in mobile cloud environments, but at the cost of privacy and model sophistication concerns. Finally, an end-to-end solution combines DL-dependent user authentication, hybrid encryption, and blockchain for safe data storage, effective task offloading in mobile edge computing with robust security layers but high system overhead and implementation complexity.

III. PROPOSED METHODOLOGY

The proposed methodology combines the Boundary-Integrated Neural Network (BINN) with TEA to achieve data security in CCE. The system functions in three broad stages such as user registration, intrusion prevention, intrusion detection. During user registration, valid users are verified and allocated access credentials. At the intrusion detection phase, BINN classifier scrutinizes cloud data access patterns to identify and predict high-accuracy unauthorized access attempts. Upon detecting suspicious activity, the intrusion prevention mechanism is triggered to deny access. At the same time, TEA makes sure that data is encrypted when stored and transmitted, offering a strong layer of protection against both internal and external attacks. This two-pronged strategy of intelligent access monitoring and robust encryption strengthens the security framework of cloud systems, providing better performance and security compared to conventional approaches. Block diagram ofSEF-CCE-BINN is represented by Fig. 1.

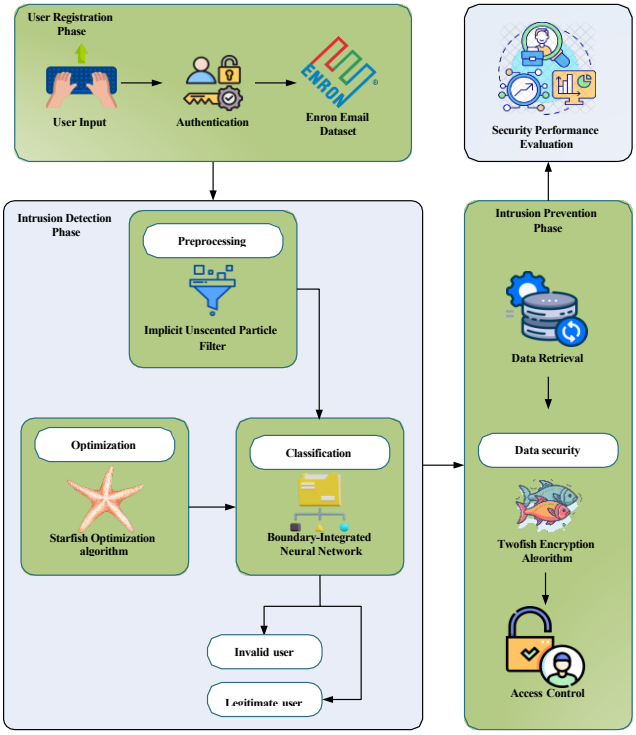

Fig. 1. Block diagram of the proposed SEF-CCE-BINN method

B. Data Acquisition

This experiment is grounded on Enron Email Dataset [16], which holds 200,399 interactions involving 158 individuals As our corpus, we used the real-life dataset, Enron email dataset. We analyze a portion of the Enron data's emails. This data is appropriate as it can cover businesses need to occasionally browse through encrypted emails are housed on far-off server. Prior to testing, we generated keywords and variations to pre-process the corpus. For keyword creation, we created inverted index for 1500 most common keywords, removed content-irrelevant terms with a spelling checker, specially cleaned up corpus utilizing Porter stemming approach. The prefix approach was used to create the permutation.

C. Preprocessing Using Implicit Unscented Particle Filter

In this section, Implicit Unscented Particle Filter (IUPF) [17] is discussed. IUPF is used for data normalization, data conversion, data sanitization in a collected data. The IUPF improves intrusion protection in cloud environment by increasing tracking accuracy and Data sanitization. It outperforms traditional filters by effectively handling nonlinear and non-Gaussian uncertainty. Furthermore, IUPF minimizes computing complexity by efficiently propagating particles, resulting in faster and more accurate disease classification. The primary purpose of IUPF in plant leaf disease detection is to track disease progression accurately and in real time. It seeks to improve diagnosis accuracy by eliminating uncertainty and improving feature extraction from complicated picture collections. Furthermore, IUPF attempts to improve computational economy while maintaining high detection performance in actual agricultural applications. The inertial navigation system in state of moment is given in equation (1),

$$\square\ Pos_e\ \square\ \square\ Pos_y\ \square$$

represents the target solution. The boundary integration is given in equation (5),

$$E_n\ \square\ \square\square\ INS^{O}\ \square 1\square\square 0\square\ \square 1\square\square vel_e\square\ w_2\ \square z_1, z_2\ ,\ y,$$

$$d\square\square\square\ \ y\square\square b\square\square d\square_{vel} INS\ \square_{k}\square 1\quad 2kk2\ \square\square y\square\square\ (1)\ (5)$$

Where E_n represents initial state velocity, Pos_e Where w represents the neural unit, $_{y}\square 1\square$ represents represents the horizontal coordinates of approximate $2k$ location of INS at current moment,

Pos_{y} represents the boundary elements, □1□ 2represents interpolation points of vertical coordinates of approximate I location. NS in current boundary elements. Even though these matrices are smaller, moment,

vel^{INS} represents the current lateral, vel^{INS} employing direct solvers necessitates a large amount of memory and computing work. It is given in equation (6), represents the longitudinal velocities. The initial moment of □0□□0□□0□□0□location is given in equation (2),

$\hat{E}_n$ □ G□E_n □ (2) b_k□ y_{k1} z_1 □ y_{k2} z_2 □ d_k (6)

Where

$\hat{E}_n$ represents the error augmented matrix, G□E_n □

Where

□0□k1represents the unknown traction vector, □0□k represents the direction cosine matrix. The velocity of the state is given in equation (3), represents the network input variable. The BINN weight parameter □ and w_1 is optimized by starfish optimization R_n □ G□E_n □ $\hat{E}_n$□□E_n □ $\hat{E}_n$□ algorithm for accurate prediction. Ultimately, the BINN was categorized as legitimate user and invalid user. The BINN method optimizes the BINN optimum parameters (3) ^{h} *and* a^{z} using SOA is used to adjust the BINN weight

Where

R_n represents the covariance of the state estimates, parameter.

G represents the attitude vector of Euler angle. Finally, data normalization, data conversion, data sanitization from the collected data was completed. Then pre-processed image fed to classification phase.

D. Classification Using Boundary-Integrated Neural Network

In this section, Boundary-Integrated Neural Network (BINN) [18] is discussed. BINN is used to classify such as legitimate user and invalid user. A BINN improves edge preservation, resulting in more accurate lesion identification. It decreases false positives and improves segmentation performance, resulting in more accurate illness categorization. It also enhances resistance to fluctuations in lighting, background noise, and leaf orientations, making it appropriate for real-world agricultural settings. The fundamental purpose model is to obtain greater accuracy in plant leaf diseases detection and categorization by incorporating boundary information into neural network processing. Finally, it aims to promote precision agriculture

E. Optimization Using Starfish Optimization Algorithm

Here, the Starfish Optimization Algorithm (SOA) [19] is introduced, which optimize the parameters □ and w_1 of BINN. Starfish, commonly called sea stars, are marine invertebrates classified as echinoderms in the class Asteroidea. The distinguishing star-like appearance of starfish is attributed to their core disk and five arms. Globally, there are about 2000 species. The number of limbs on other starfish species can range from 7 to more than 10. Although they can range from 0.5mm to more than 50cm, their sizes typically fall between 12 and 25 cm. Because they lack osmoregulation, starfish are mostly found in the deep sea and infrequently in freshwater. It lives for ten years, although some can reach 35 years.

Step 1: *Initialization*

During the initialization phase of SOA, starfish locations are generated at random based on design variables and expressed as a matrix is given in equation (7), by enabling early disease identification, lowering crop losses, and assisting farmers in timely intervention. The displacement component is given in equation (4),

$$Y_{11} \quad Y_{12} Y \quad Y_{Y} \square \quad \square \quad 21 \quad 22 \square \quad Y_{1E} \square$$
$$Y_{2E} \quad (7)\ w\ (z, z\ , y, d)\ ^{O}_{y} \square 1 \square\ (\ \square 0 \square) \square 1 \square :$$
$$\vdots \quad \ddots \quad \vdots \ 11 \quad 2 \square \square k \square 1\ (4)\ \square Y_{O1}$$
$$Y_{O2} \quad O \square E$$

Where d □1□ represents the b □0□ represents the weights that Where Y represents the matrix to save starfish positions based on size, O □ E represents the population size, connect the kth neural unit to the input data, □1□1k

Step 2: *Random Generation*

Input parameters are created at random. Optimal fitness represents the weights of the target solutions from the jth neural unit, □ represents the activation function, w_1 value is chosen based on obvious hyper parameter circumstances.

Step 3: *Fitness Function*

It generates random solution from initialization and expressed in eqn (8),

Fitness function □ *Optimizing* (□ *and* w_1) (8)

Where □ is employed for increasing the accuracy; and w_1

is utilized to utilized for reducing f1 score.

Step 4: *Exploration phase*

The exploration stage of SOA algorithm is utilized for simulating starfish behavior, which simulates the exploring capacity of five arms with eyes inserted at

the ends. It is given in equation (9), $Z^u \; Y^u \; b$ $(Y^u \; Y^u) \cos, s \; 0.5 \; j, q \; j, q1 \; best, q \; j, \; q$ $\{Z^u Y^u \; b \; (Y^u \; Y^u) \sin, s \; 0.5 \; j, q \; j, \; q$ 1 $best, q j, q$ (9) U Where $Z_{j,\,q}$ represents the obtained position of the starfish, Uj, q represents the current position of the starfish, $Y^{U}_{best,q}$ represents the dimension of the position, q represents the selected dimension.

Step 5: *Exploitation phase*

SOA evaluates predatory and regeneration behaviours' throughout the exploitation period to propose global solutions. This includes constructing two updating techniques. Using a simultaneous two-directional search approach that considers data from other starfish as well as the population's current ideal location, SOA simulates the preying phase of starfish. It is given in equation (10), $e_n \; (Y^u \; Y^u)$ (10)

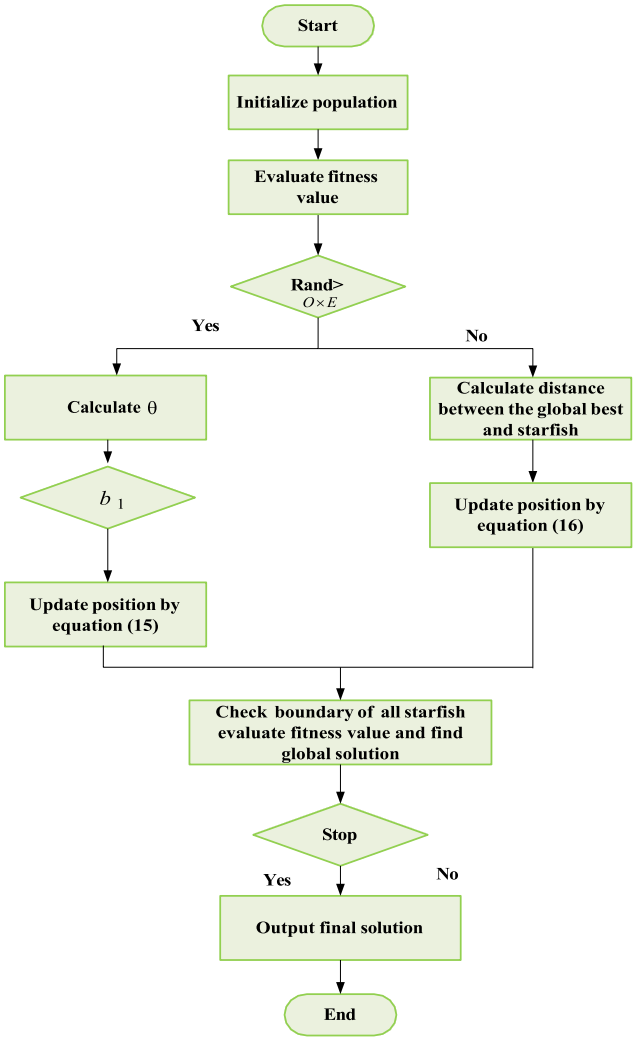

Fig. 2. Flow chart of SOA

Where

e_n represents the global best starfish, n_q represents

F. Data Security Utilizing Twofish Encryption Algorithm

A TEA is utilized to encrypt data entered following randomly chosen starfish.

Step 6: *Termination criteria*

The weight parameter of and w_1 generator from BINN registration. The TEA [20] is a symmetric key cryptography algorithm. The key length of 64-bit block ranges from 32 to 448 parts. A P-array with four 32-bit S-boxes are offered. While conveying 32-bit yield, the S-boxes are able to are enhanced using SOA process; iteratively repeat step 3 halting conditions $Y \; Y \; 1$. Then finally BINN for plant leaves disease classification with better accuracy and lower f1 score. Figure 2 shows flow chart of SOA. recognize 8-bit data. The two main steps of the TEA are the encryption and key expansion phases. To encrypt information, 16-round FSTEL network is used. In every round, main dependence permutations and key-dependent substitutions are carried out. The addition of 32-bit words is the only

operation in XOR and BA. Fig. 3 illustrates structure of TEA.

Swap Y_M *and* Y_S

Next l

Swap Y_M *and* Y_S (undo the last swap)

$Y_s = Y_s XOR_{q17}$

$Y_M = Y_M XOR_{q18}$

Re *merge* Y_M *and* Z_S

$Q1$ $Q2$

Algorithm 1 illustrates the Two fish encryption algorithm by algorithm Function that is defined below.

$g\ (YM)$ □((T, j □T, k mod 2^{32}) XORT, l) □T, m mod 2^{32}o0123 (14)

Divide Partition Y_M, into 8-bit segments: j, k, l, m

$Q16$

$Q12$ $Q18$

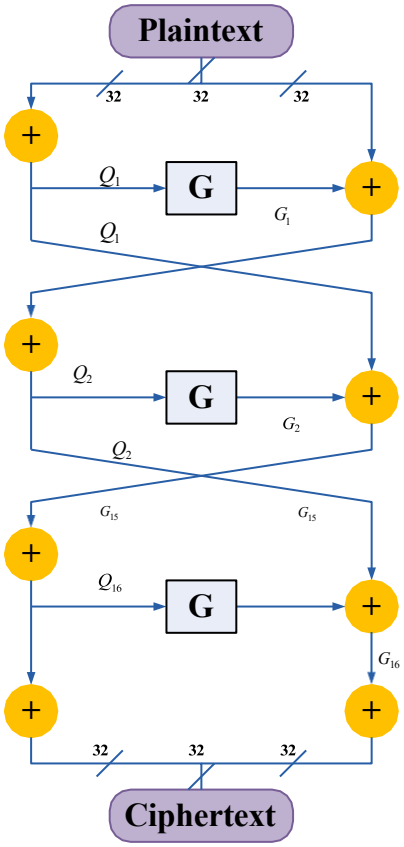

Fig. 3. Structure of TEA

1) Public Key Encryption Process:

At this stage, the key for authorized access is generated by the data owner using an elliptic algorithm. Then, Twofish is used to encrypt the records and index.

Step 1: *Keys' Conception*

ECC's beginning is data given below.

F: y^2 □x^3 □bz □d (11)

$4b^3$ □ $27c$ □ 0 mod s (12)

Here, b and c are integers fulfilling condition (11), s denotes prime, s contains point at infinity.

Q □e*s (13)

Where, e is an arbitrary number among 1 and n □1. s for curve's point, e for private key, Q for public key.

Step 2: *maintaining personal data*

The Twofish approach is employed to resolve privacy issues. This symmetric block cipher is suitable for encrypting and storing data.

Algorithm 1: Twofish encryption algorithm

Split Y into 32-bit division: Y_M, Y_S

For $l = 1 to 16$

$Y_M = Y_M XOR_{ql}$

$Y_s = G\ (Y_M) XOR_{YS}$

Step 3: *Cloud storage*

For convenience of information owner, searchable index J, collection of system files D are stored in cloud. The index locates the relevant encrypted data after receiving user's query request and makes it available to users. An authorized user creates query request with sends it to cloud server when they need to know something about the cloud data. The cloud server processed request after receiving encrypted text, using cloud's index to create paired outcomes. The cloud server's database utilities are then decrypted by the authorized user.

T [0]: 243f6a88	**T [9]: 38d01877**
T [1]: 85a368d3	T [10]: be5466cf
T [2]: 13198a2e	T [11]: 34e90c6c
T [3]: 03,707,244	T [12]: c0ac24b7
T [4]: a4093822	T [13]: c97c50dd
T [5]: 279f31d0	T [14]: 3f87d5b5
T [6]: 082efa98	T [15]: b5470517
T [7]: ec4e6c89	T [16]: 9296d5d9
T [8]: 452821e6	T [17]: 8879fb1b

G. Data Retrieval

Twofish encryption-based intrusion prevention incorporates a set of steps for the safe retrieval of data and access control. When a valid request for data is sent, the system gets back the data that has been encrypted. The Twofish encryption method is utilized to check the validity of the request through encrypting and decrypting the data to ensure the request is coming from an authenticated user. If the credentials of the user are successfully authenticated, the data is decrypted and authorized for retrieval. But if the authentication is unsuccessful or the request is unauthorized, access to the data is blocked so that sensitive information is not exposed to

unauthorized access or intrusion.

IV. RESULT AND DISCUSSION

Java coding is employed to execute the proposed full-text search method. On a Windows 7 server with 64-bit 2.9 GHz processor, 4 GB of main RAM, it were performed. Decryption time, Encryption time, accuracy, recall are analyzed to establish how robust proposed coding system is. It is accepted to confirm proposed method. It was contrasted with the other genetic data encryption, current encrypted using symmetric keys methods with respect to encryption time, recall, decryption time and accuracy in relation to scope of plain text, required time for encryption with decryption.

A. Performance Measures

Accuracy and recall is employed to estimate the effectiveness of proposed approach.

1) *Accuracy:* The rate of correctly classified detections is referred to as accuracy. Equation (15) is where the formula is derived. is analyzed with existing SEF-CCE-LSTM, SEF-CCE-KMA and SEF-CCE-TTTD methods respectively.

Accuracy □□*TP* □*TN* □

TP □ *FP* □ *TN* □ *FN* (15)

Where, *TP* signifies True Positive, *TN* signifies True Negative, *FP* signifies False Positive, *FN* signifies False Negative.

2) *Recall:* In binary classification tasks, such as medical exams, where objective is to exactly detect negative cases, recall is a performance metric that is frequently used. Equation (16) is then used to derive the formula.

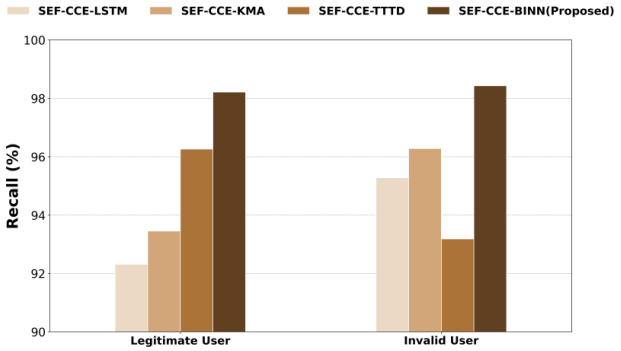

Fig. 5. Recall analysis

Fig. 5 depicts recall analysis. The graph is given between the recall percentages of various models that have been made to separate valid and invalid users. Models used are SEF-CCE-LSTM, SEF-CCE-KMA, SEF-CCE-TTTD, and SEF-CCE-BINN (Proposed). For valid users, the recall rates are nearly the same for all the models, with the proposed SEF-CCE-BINN having the highest recall rate of close to 98%. On the other hand, the recall of invalid users is slightly

Recall □ TN □*FP* □*TN* □(16)

lower but equally impressive, with the suggested model also performing the best in this category. Generally, the graph illustrates the efficiency of the suggested SEF-CCE-BINN model in having high recall rates for both legitimate and

B. Performance Analysis

Fig. 4-7 shows simulation outcome of SEF-CCE-BINN technique for Level of automation. The performance metrics are analyzed with existing techniques such as SEF-CCE-LSTM, SEF-CCE-KMA and SEF-CCE-TTTD methods.

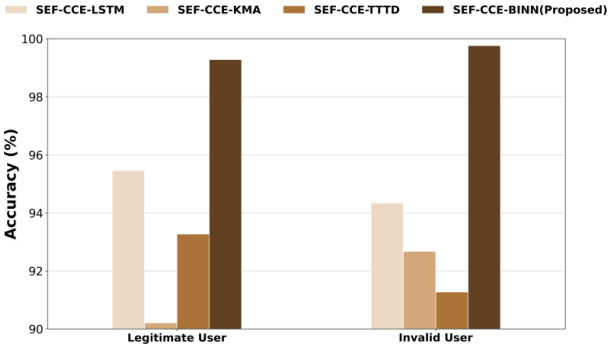

Fig. 4. Accuracy analysis

Fig. 4 depicts accuracy analysis. The graph gives a comparison of accuracy percentages among various models SEF-CCE-LSTM, SEF-CCE-KMA, SEF-CCE-TTD, and the proposed SEF-CCE-BINN in detecting legitimate and invalid users. The models are indicated by varying shades of brown, and the proposed model (SEF-CCE-BINN) has the highest accuracy for both classes. For legitimate users, all models have high accuracy, but the proposed model is superior by achieving almost 100%. For invalid users, the suggested model is also much more accurate than the rest, suggesting that it performs well in identifying both valid and invalid users correctly. Generally, the SEF-CCE-BINN method performs better than all the other methods in this regard. The SEF-CCE-BINN attains 17.84%, 23.23% and 32.82% higher accuracy for Semi-automatic and 17.02%, 24.63% and 32.82% higher accuracy for Automated which invalid users in comparison to the other models. The SEF-CCE-BINN attains 18.14%, 23.84%, 32.77% greater recall for Semi-automatic and 16.98%, 23.32%, 30.30% greater recall for Automated that is analyzed with existing SEF-CCE-LSTM, SEF-CCE-KMA and SEF-CCE-TTTDmethods respectively.

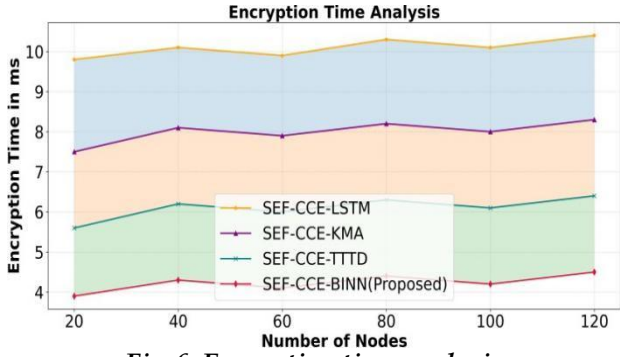

Fig. 6. Encryption time analysis

Fig. 6 depicts encryption time analysis. The graph compares the encryption times (in milliseconds) across different algorithms (SEF-CCE-LSTM, SEF-CCE-KMA, SEF-CCE-

TTTD, and SEF-CCE-BINN Proposed) as the number of nodes increases from 20 to 120. Each algorithm shows distinct performance trends, with the SEF-CCE-BINN (Proposed) demonstrating consistently lower encryption times than the other methods across most node counts. The SEF-CCE-LSTM and SEF-CCE-KMA exhibit similar performance, while SEF-CCE-TTTD tends to have higher encryption times, especially at lower node counts. Overall, the graph suggests that BINN method is more efficient regards encryption time as the network scales.

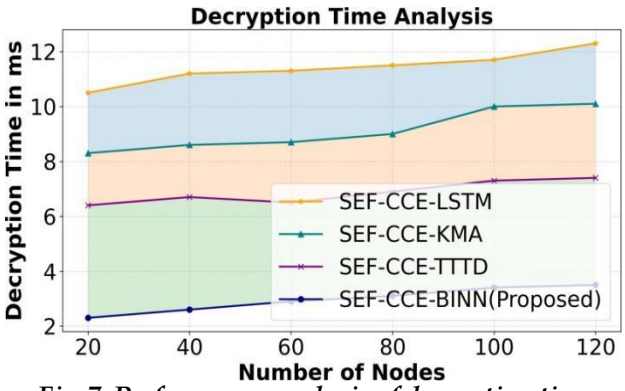

Fig. 7. Performance analysis of decryption time

Fig. 7 depicts decryption time analysis.The graph illustrates the relationship between the number of nodes and the decryption time measured in milliseconds (ms) across four different methods: SEF-CCE-LSTM, SEF-CCE-KMA, SEF-CCE-TTTD, and SEF-CCE-BINN (Proposed). As the number of nodes increases from 20 to 120, the decryption time generally trends upward for all methods, with SEF-CCE-BINN (Proposed) exhibiting the lowest decryption times compared to the other methods. The SEF-CCE-LSTM method shows the highest decryption times, particularly as the number of nodes approaches 120. The shaded areas in the background may indicate ranges of variability or confidence intervals for the different methods, emphasizing the relative efficiency of the proposed method in handling larger node counts. Overall, the graph effectively demonstrates that the proposed SEF-CCE-BINN method consistently outperforms its counterparts in terms of speed.

C. Discussion

The addition of Boundary-Integrated Neural Network (BINN) and Twofish Encryption Algorithm (TEA) provides an effective remedy to the current challenge of safeguarding confidential data in cloud computing. With the virtual world depending more on distributed systems, data during transmission and storage must be secured, even with the inherent vulnerability of internet-based access. The introduced three-phase process user authentication, intrusion detection, and intrusion blocking triggers a multifaceted scheme to cloud protection. BINN is successful in identifying and foreseeing unauthorized accesses patterns, and TEA grants only authenticated users access to the cloud-stored data via heavy encryption. From the comparative overview against current classifiers, it transpires that the SEF-CCE-BINN process improves notable anomaly detection with stronger data covertness. Experimental results show not only enhanced execution efficiency but also a significant increase in overall security of data, substantiating the system's value as a reliable framework for protecting cloud applications.

V. CONCLUSION

In summary, the combination of the Boundary-Integrated Neural Network (BINN) and the Twofish Encryption Algorithm (TEA) is a very efficient system for protecting cloud computing systems from unauthorized use and possible cyber-attacks. The multi-stage method of the proposed system covering user registration, intrusion detection, intrusion prevention exhibits robust capability in precise anomaly detection and protection of data integrity. Experimental evaluation ensures that the SEF-CCE-BINN algorithm is effective in promoting security measures and execution efficiency compared to other solutions. Future directions can include applying this framework to large-scale, real-time cloud environments, incorporating adaptive machine learning models that adapt as new threats are learned, and investigating lightweight encryption methods to optimize security and performance in low-resource systems like edge computing and IoT-based clouds.

REFERENCES

[1] Salvakkam, D.B., Saravanan, V., Jain, P.K. and Pamula, R., 2023. Enhanced quantum-secure ensemble intrusion detection techniques for cloud based on deep learning. Cognitive Computation, 15(5), pp.1593-1612.

[2] Rajeshkumar, K., Dhanasekaran, S. and Vasudevan, V., 2024. Efficient and secure medical big data management system using optimal map-reduce framework and deep learning. Multimedia Tools and Applications, 83(16), pp.47111-47138.

[3] Alzoubi, Y.I., Mishra, A. and Topcu, A.E., 2024. Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57(5), p.132.

[4] Sucharitha, G., Godavarthi, D., Ramesh, J.V.N. and Khan, M.I., 2024. Secure and efficient content-based image retrieval using dominant local patterns and watermark encryption in cloud computing. Cluster Computing, 27(9), pp.11873-11889.

[5] Preethi, B.C., Vasanthi, R., Sugitha, G. and Lakshmi, S.A., 2024. Intrusion detection and secure data storage in the cloud were recommend by a multiscale deep bidirectional gated recurrent neural network. Expert Systems with Applications, 255, p.124428.

[6] Umar, T., Nadeem, M. and Anwer, F., 2024. Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage. Expert Systems with Applications, 257, p.125050.

[7] Kumar, A. and Kumar, S., 2024. An Advance Encryption and Attack Detection Framework for Securing Smart Cities Data in Blockchain Using Deep Learning Approach. Wireless Personal Communications, 135(3), pp.1329-1362.

[8] Kumar, A., Khan, S.B., Pandey, S.K., Shankar, A., Maple, C., Mashat,

A. and Malibari, A.A., 2023. Development of a cloud-assisted classification technique for the preservation of secure data storage in smart cities. Journal of Cloud Computing, 12(1), p.92.

[9] Chatterjee, P., Bose, R., Banerjee, S. and Roy, S., 2023. Enhancing data security of cloud based lms. Wireless Personal Communications, 130(2), pp.1123-1139.

[10] Kanagala, P. and Jayaraman, R., 2023. Effective encryption approach to improving the secure cloud framework through fuzzy-based encrypted cryptography. Soft Computing, pp.1-10.

[11] Suganya, M. and Sasipraba, T., 2023. Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment. Journal of Cloud Computing, 12(1), p.74.

[12] Ahmad, S., Mehfuz, S., Urooj, S. and Alsubaie, N., 2024. Machine learning-based intelligent security framework for secure cloud key management. Cluster Computing, 27(5), pp.5953-5979.

[13] Akbar, M., Ahmad, I., Mirza, M., Ali, M. and Barmavatu, P., 2024. Enhanced authentication for de-duplication of big data on cloud storage system using machine learning approach. Cluster Computing, 27(3), pp.3683-3702.

[14] Wang, Y., Chen, L., Wu, G., Yu, K. and Lu, T., 2023. Efficient and secure content-based image retrieval with deep neural networks in the mobile cloud computing. Computers & Security, 128, p.103163.

[15] Ganesh, N.S., Balasubramanian, V., Prasad, D. and Velan, S.S., 2025. Deep learning-based user authentication with hybrid encryption for secured blockchain-aided data storage and optimal task offloading in mobile edge computing. Wireless Networks, 31(3), pp.2389-2417.

[16] https://www.kaggle.com/datasets/wcukierski/enron-email-dataset

[17] Cheng, L., Zhao, Z., Shi, Y. and Lu, Y., 2024. Implicit unscented particle filter based indoor fusion positioning algorithms for sensor networks. Alexandria Engineering Journal, 94, pp.104-119.

[18] Zhang, P., Xie, L., Gu, Y., Qu, W., Zhao, S. and Zhang, C., 2024. Boundary integrated neural networks for 2D elastostatic and piezoelectric problems. International Journal of Mechanical Sciences, 280, p.109525.

[19] Zhong, C., Li, G., Meng, Z., Li, H., Yildiz, A.R. and Mirjalili, S., 2025. Starfish optimization algorithm (SFOA): a bio-inspired metaheuristic algorithm for global optimization compared with 100 optimizers. Neural Computing and Applications, 37(5), pp.3641-3683.

[20] Sathish, B. and Anithaashri, T.P., Analyzing security vulnerabilities in consumer IOT applications using Twofish encryption algorithms comparing with DES algorithm. In Applications of Mathematics in Science and Technology (pp. 970-973). CRC Press.