International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 1135-1154
https://doi.org/10.70917/ijcisim-2026-2447
Article

Blockchain-Enabled Maximum Support Deep Belief Neural Network Technique for Cyber Threat Detection in the Financial Sector

R.Saranya[1*], Sumathy Kingslin[2]

[1*] PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (A), Chennai - 600002, Tamil Nadu, India.
[2]PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (A), Chennai -600002, Tamil Nadu, India.
Email: rsaranya.research@gmail.com.

Abstract: The increasing digitisation of financial transactions has led to a growing vulnerability to cyber threats, including fraud, unauthorised access, and data breaches. Existing approaches for detecting financial threats suffer from several issues, including low detection rates due to data imbalance, insufficient feature selection methods, and the inability to extract subtle transactional patterns. However, the lack of integrated frameworks that combine smart detection with encryption and access control in existing security solutions makes these solutions susceptible to advanced cyberattacks. To overcome these problems, the proposed Blockchain-enabled Maximum Support Deep Belief Neural Network (MSDBN2) technique is used to detect cyber threats in the financial sector. The Malicious Activity Prone Factor (MAPF) scheme is used to analyze the behaviour of processes from a collective dataset. Then, the Optimized Dragon Fly with Decision Tree (ODF-DT) approach is used to select the essential features of financial cyber threats. After that, the proposed MSDBN2 approach learns the complex patterns and correlations of the selected features. Here, the Maximum support weight vectors determine the optimal hyperplane that separates normal from threat classes. Based on threat detection, the Circular Shift Elliptic Curve Data Encryption (CSECDE) method encrypts the financial information. Next, the Blockchain-based Dynamic Chain Link Policy (BDCLP) scheme is used to prevent unauthorized access. Finally, the Quantum Key Authentication (QKA) technique is employed to verify the authorized users in the financial sector. Therefore, the proposed method achieves higher security performance and threat-detection accuracy than other methods. The proposed model is assessed using several performance metrics, including accuracy, precision, recall, F1-score, time complexity, encryption and decryption efficiency, authentication performance, and security performance. The experimental results reveal that the proposed approach achieves 96.72% accuracy and 96.10% improved security performance.
Keywords: Cyber Threat Detection, Blockchain Security, Deep Belief Neural Network, MSDBN2, Feature Selection, Dragonfly Optimization, Elliptic Curve Encryption, Quantum Key Authentication, Data Security, and Fraud Detection.

1. Introduction

In today's world, Artificial Intelligence (AI) is a key enabler of modern cybersecurity, offering advanced threat detection, analysis, and risk evaluation and using blockchain technology and AI methodologies to enhance security and privacy, enabling decentralized, immutable data storage solutions. Additionally, AI-based attacks can affect availability, confidentiality, and integrity. AI systems play a crucial role in detecting and mitigating the rapidly emerging risks posed by such attacks in real-time. Additionally, AI technology facilitates the analysis of massive datasets, enabling the identification of trends and the detection of anomalies that may signal potential cyber threats.

Efficient finance promotes the development of the financial system by adopting modern digital technology and by being more efficient, undertaking fewer transactions, and incurring lower financial cost. Transparency based on blockchain enables the production of traceable, immutable, and auditable records. This reduces information asymmetry, increases trust, and minimises the risk of fraud and fraudulent advertising in the sustainable finance industry. By continuously analysing several data sources, AI-driven analysis and real-time monitoring enhance risk management, fraud detection, and proactive compliance [2]. Furthermore, digital payment infrastructure and smart contracts can enable more rapid and extensive financial services, ease operational constraints, and accelerate cross-border transactions.

Additionally, the financial industry has long been a focus of security concerns, with commercial banks

particularly susceptible to cyber-attacks given the significance of transaction and client data [3]. The effect of blockchain technology on reducing cybersecurity risks in financial transactions at commercial banks. Because blockchain technology can completely transform the financial industry by enhancing security, efficiency, and transparency, it is quickly gaining global interest. Blockchain technologies are being adopted by financial institutions worldwide to modernise business processes, reduce operational risk, and enhance security against cyberattacks.

However, due to their evolution, these networks are vulnerable to fraud, necessitating advanced security and reliability methods [4-5]. Identity theft, money laundering, and payment fraud are just a few of the dishonest tactics used in financial networks to exploit weaknesses and profit. Conventional fraud detection techniques, including rule-based systems, often lag as fraud activity becomes more complex. This leads to problems such as low efficiency, high false-alarm rate, and difficulties with real-time detection. However, this integration also poses significant cybersecurity risks that may undermine user confidence, operational reliability, and data integrity. Customised cybersecurity risk assessment frameworks that account for these distinctive features are more important than ever as the use of blockchain in the financial technology industry continues to grow.

The primary contribution of the research is the design of a multi-layered cybersecurity model for financial systems that combines intelligent cyber threat detection with effective data security. The framework proposes the MAPF scheme to process and understand the behavioural patterns in financial transactions, followed by an ODF-DT scheme for optimal feature selection. The proposed blockchain-based MSDBN2 is designed to learn complex patterns in data and enhance the accuracy of cyber threat detection. To enhance security, the model also includes CSECDE for secure data sharing, as well as a BDCLP to protect against data theft and ensure data integrity. Additionally, QKA enhances user authentication and security.

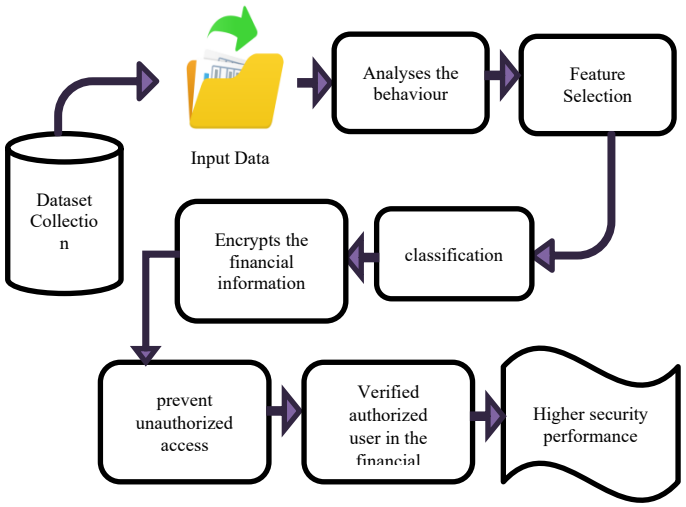

Fig. 1. Basic Diagram for Cyber threat detection in the financial sector

Figure 1. Framework for cyber threat detection in the financial sector. The data is collected and analysed, features are selected, and classification is performed to detect cyber threats. Data safety is maintained through user authorization and encryption. So, it is done by analysing data that only authorized users can access, which enhances its performance.

2. LITERATURE SURVEY

To safely capture and permanently store AI-generated alerts and related metadata, this research [6] designed an integrated system that combines a Convolutional Neural Network (CNN)-based anomaly detection module with the permissioned Ethereum blockchain. Traditional cybersecurity methods often lack consistency and exposure in documenting and validating AI outcomes. This research presented a comprehensive examination of AI-supported threat-detection algorithms in blockchain-based systems [7]. However, as the blockchain ecosystem grows, more complex cyber threats are emerging, posing risks to the network's security, privacy, and integrity.

To provide reliable fraud detection in financial transactions, this study [8] investigates integrating lightweight blockchain technology with Deep Learning (DL). By ensuring that transactions and data sharing between nodes are transparent and immutable, lightweight blockchains address reliability and security issues. This novel [9] described the significance of explainable AI (XAI) for enhancing the accountability, transparency, and dependability of AI-based fraud detection systems. However, the rise in illicit activity and fraudulent transactions

has also coincided with the expansion of digital currencies.

TABLE I: CYBER THREAT DETECTION IN THE FINANCIAL SECTOR USING DL ALGORITHM

Author(s)	**Year**	**Classification Method Name**	**Dataset Used**	**Limitations**
Bello [13]	2022	Generative Adversarial Networks (GANs)	Financial transaction datasets (unspecified)	Lack of dataset transparency and limited real-time validation
Almahadeen [14]	2024	Auto Encoder-Multilayer Perceptron (AE-MLP)	Financial cybersecurity dataset	Computational complexity and risk of over-fitting
Udayakumar [15]	2023	Deep Fraud Net	Cyber fraud datasets	Limited generalization
Darem [16]	2023	Threat Classification Framework	Banking and financial sector data	Lacks experimental validation
Rajkumar [17]	2025	Gaussian Encoder Belief Network (GEBN).	Banking monitoring datasets	High computational cost
Li [18]	2022	Deep Auto-Encoder - LSTM (DAE -LSTM)	Financial credit datasets	Complex architecture and long training time
Kumar [19]	2024	Modified Deep Neural Network (M-DNN)	Smart city datasets	Integration complexity and high implementation cost
Mulea [20]	2025	Multi-Layer Perceptron Neural Network (MLPNN)	Banking sector data	Limited benchmarking, lacks comparison with baseline models

Table 1 demonstrates that the classification from the prior set using the DL approach, dataset, and the limitation was also used to identify cyber threats in the financial industry. To address these financial transition issues, this paper [10] employed blockchain-based financial technology in the banking industry. This research

Demonstrates the performance of the proposed Adaptive Neuro-Fuzzy K-Nearest Neighbour (ANF-KNN) algorithm by comparing it with some other methods. The blockchain guarantees the validity, integrity, and traceability of model changes, and the suggested framework enables collaborative learning of intrusion detection models without sharing the original data. To identify complex attack patterns against distant nodes, this paper [11] employs a DL model based on a Long Short-Term Memory (LSTM) network. By providing real-time monitoring and early threat mitigation, this novel [12] proposed a Support Vector Machine (SVM)- based framework that enhances the security of digital banks, protects sensitive financial information, and maintains client trust. However, financial institutions are now vulnerable to several attacks and face serious cybersecurity difficulties as a result of this digital revolution.

TABLE II: BLOCK CHAIN-BASED CYBER THREAT DETECTION IN SECURE FINANCIAL TRANSACTION

Author	**Year**	**Classification Methods**	**Financial Type**	**Performance Metrics**	**Drawbacks**
Tolah, A. [21]	2025	Zero-Knowledge Proofs (ZKP)	Banking & Financial Networks	Accuracy, latency, throughput	Scalability issues; high storage overhead; limited real-time adaptability
Goundar [22]	2025	CNN	Digital Payments & Online Banking	Accuracy, response time, detection rate	Complex system design; integration challenges; computational overhead

Kumar [23]	2024	Parallel Stacked LSTM (PSLSTM)	Financial Decision Systems	Precision, Recall, F1-score	Increased model complexity; slower processing due to explain ability layer
Shukla [24]	2024	Random Sequence-Based Symmetric Encryption (RSBSE) algorithm	Cyber-Physical Financial Infrastructure	Encryption efficiency, security strength	Limited applicability to pure financial datasets; key management issues
Chaudhry & Hydros [25]	2023	Zero-Trust Security Model (ZTSM)	Banking Systems	Accuracy, breach detection rate	High computational cost; latency in consensus mechanisms
Mohamed Iliyas [26]	2025	Elliptic Curve Cryptography (ECC)	Financial Transactions (Block chain-based)	Security level, encryption time, transaction efficiency	Complex implementation; high cryptographic computation cost
Vatambeti [27]	2022	Light-Weight Block chain-Based Signature Algorithm (LWBSA)	Banking & Secure Transactions	Efficient attack detection and secure authentication	Limited scalability; constrained performance
Rane [28]	2023	Multi-Factor Authentication (MFA) technique	Modern Banking Systems	Improving transaction transparency	Mostly conceptual analysis; lacks experimental validation

As shown in Table 2, the classification methods of the block chain-based cyber threat detection system are based on the previous research, including the financial classification, the performance metrics, and the recognized limitations, to enable secure financial transactions.

The advantages of both technologies are used in the suggested framework to increase stakeholder confidence and detection accuracy [29]. A detection accuracy of 96.4% was observed in experimental assessments conducted in a block chain simulation. The result is that block chain is far more secure for transactions, AI-based fraud detection achieves 92% accuracy, and biometric authentication is proven to tighten access control. This paper [30] the authors propose conclude that the combination of block chain and AI-based cyber security solutions provides a strong means of enhancing trust and security in the digital financial industry.

A. Problem Statement

The growing number of transactions in the financial industry has resulted in a dramatic increase in cyber threats including fraud, data breaches and access control. Current cyber threat detection approaches have several issues, such as poor detection accuracy, which is partly caused by extremely imbalanced data, sub-optimal feature selection and the inability to effectively capture complex transaction patterns. Moreover, existing systems are primarily focused on detection and do not incorporate security measures, such as encryption, access control, and user authentication, thus exposing them to sophisticated cyber threats.

Moreover, lack of decentralized security mechanisms also raises concerns of data manipulation and tampering. Consequently, there is a pressing need for an intelligent, secure, and integrated framework capable of predicting cyber threats and ensuring data confidentiality, integrity, and authentication in financial systems.

B. Objective of the research

The main objective of this research is to design an effective and efficient Block chain-based MSDBN2 framework for cyber threat detection in the financial industry. To propose a MAPF approach to model financial

data behaviour and accurately detect threats. To develop an ODF-DT method for feature selection to enhance model efficiency and reduce complexity. To improve threat detection accuracy by using the MSDBN2 model to capture the relationships of the data. Furthermore, to secure data transmission with CSECDE, unauthorized access with a BDCLP, and user authentication with QKA. Furthermore, the goal is to develop a comprehensive methodology that enhances threat detection, data security, and system reliability beyond existing methods.

3. PROPOSED METHODOLOGY

This section proposes an approach to financial cyber threat detection that integrates feature analysis, optimization, DL, encryption, and blockchain security. The MAPF scheme detects transaction patterns, ODF-DT determines features, and the MSDBN2 accurately classifies threats. Lastly, the CSECDE encryption algorithm, BDCLP blockchain policy, and QKA authentication provide data security and access control.

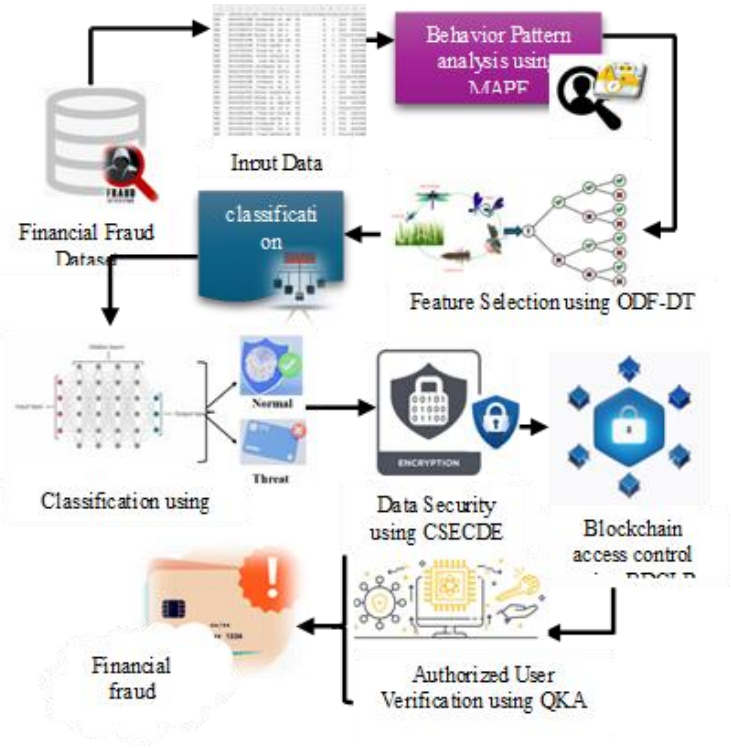

Fig. 2. Proposed MSDBN2 method based on the architecture diagram

The proposed system architecture in Figure 2 addresses fraud detection in the blockchain-based financial sector by combining sophisticated machine learning techniques with security measures. The first step is the financial fraud data, which is the input data containing normal and fraudulent financial transactions. First, the Malicious Activity Prone Factor (MAPF) scheme conducts behavioural pattern analysis by examining various transaction features, including volume, frequency, and account type, to detect unusual patterns. The pre-processed data is then fed to the Optimized Dragonfly with Decision Tree (ODF-DT) technique, which efficiently identifies the optimal features by removing redundant features and reducing the dimensionality of data for faster computation. The optimal features are then input to the MSDBN2 with multiple hidden layers that learn complex patterns and connections in the data. After classification, the system provides data security by using the CSECDE method, which encrypts and converts sensitive financial data to maintain its secrecy. After encryption, BDCLP is used to ensure secure and reliable data storage by securely linking transaction data through hash functions and using dynamic access control policies. Finally, QKA is applied to authenticate users via secure key matching, providing secure user access.

A. Dataset Collection

The Financial Fraud Detection dataset, available at https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset, is used for the experiments. The Financial Fraud Dataset is a large tabular dataset for financial fraud detection research, with 1,048,576 transactions. It emulates real-world users' activity and fraud patterns to allow researchers and practitioners to experiment with machine learning models on a safe subset of data without using sensitive real data. In this study, the dataset is split into the traditional 80:20 ratio, with 80% for training and 20% for testing. Consequently,

838,860 records are used to train the model to identify transaction patterns, user behaviours, and fraud-related anomalies. The remaining 209,716 records are held out for the testing set to evaluate the model's performance on new data.

step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest
1	PAYMENT	9839.64	C1231006815	170136	160296.36	M1979787155
1	PAYMENT	1864.28	C1666544295	21249	19384.72	M2044282225
1	TRANSFER	181	C1305486145	181	0	C553264065
1	CASH_OUT	181	C840083671	181	0	C38997010

Fig. 3. Dataset Feature collection

The dataset is highly imbalanced: it consists of financial transactions (with 11 attributes) with very few fraudulent activities, as shown in Figure 3. Fraudulent transactions are mostly found in transfer and cash-out transactions. The dataset is highly imbalanced, with the number of fraudulent transactions much smaller than that of legitimate transactions, and it is crucial that the training and testing sets maintain the same distribution.

B. Malicious Activity Prone Factor (MAPF)

The MAPF scheme is used as a preliminary behaviour analysis module in the proposed blockchain-based financial fraud detection system. It analyzes transactions from the financial dataset to detect unusual activity using features such as amount, time, and account usage patterns. The MAPF approach calculates a fraud score for each transaction based on deviations from normal transactional behaviour, indicating transactions that are more likely to be fraudulent. This process aids in pre-processing and flagging transactions for further investigation. In blockchain, MAPF improves data quality by filtering and processing only transactions that are validated and behaviorally examined. By conducting early risk assessment, MAPF increases detection accuracy, reduces false alarms, and enhances the effectiveness of the cyber threat detection system in banking applications.

As shown in equation 1, calculate the feature vector using transaction behavioural attributes such as amount, frequency, date, and balance. Let's assume X_i–transaction, A_i– Transaction amount, F_i– Transaction frequency, B_i– Balance behavior (difference between old and new balance)

$$X_i = \{A_i,\ F_i, B_i\} \tag{1}$$

As shown in Equation 2, calculate the average value of the behaviour for the transaction set to characterize the normal transaction pattern within the dataset. Let us assume μ– Mean (normal behavior), N– Total number of transactions, $and\ X_i$– Transaction feature vector.

$$\mu = \frac{1}{N}\sum_{i=1}^{N} X_i \tag{2}$$

As shown in Equation 1, calculate the deviation value of the transaction volume to detect financial fraud. Let us assume D_i– Deviation score, X_i– Current transaction, μ– Mean behavior.

$$D_i = |X_i - \mu| \tag{3}$$

The MAPF score is based on the weighted contributions of transaction amount, frequency, and deviation to estimate transaction risk, as shown in equation 4. Let's assume $MAPF_i$– Risk score of transaction, α, β, γ– Weight coefficients (importance factors), A_i– Transaction amount, F_i– Transaction frequency, D_i– Deviation

$$MAPF_i = \alpha A_i + \beta F_i + \gamma D_i \tag{4}$$

The MAPF score is used to determine whether a transaction is abnormal or normal using a threshold, as shown in equation 5. Let us assume Y_i– Output class (1 = Fraud, 0 = Normal), $MAPF_i$– Risk score, θ– Threshold value

$$Y_i = \begin{cases} 1, & \text{if } MAPF_i > \theta \\ 0, & \text{otherwise} \end{cases} \text{b} \tag{5}$$

The MAPF model assigns a risk value to a transaction based on its abnormal behaviour. If the MAPF value is greater than a certain threshold, the transaction is regarded as a fraud; otherwise, it is regarded as a normal transaction. This allows early detection of fraudulent transactions and enhances the detection of financial fraud.

C. Optimized Dragon Fly with Decision Tree (ODF-DT)

This section uses the ODF-DT approach to select the essential features of financial cyber threats. The ODF-DT algorithm is employed as a feature selection tool to select essential features for detecting financial cyber

threats. This involves the Dragonfly Optimization algorithm searching the feature space and identifying the best feature subsets according to their relevance and impact on classification accuracy. The identified features are further assessed using a Decision Tree classifier, which aids in assessing their importance through decision paths and information gain. The ODF-DT method leverages both optimization and classification methods to eliminate redundant and irrelevant features, enhance model performance, and reduce computational time. It ensures that the most relevant features are selected to move forward to the next stage of cyber threat detection.

The dataset has features F, each representing a financial transaction feature, as shown in equation 6. Let's assume F– Total feature set, f_i– Individual feature, n– Number of features

$$F = Y_i\{f_1, f_2, f_3, \ldots, f_n\} \quad (6)$$

The Dragonfly algorithm moves solutions (feature subsets) using swarm intelligence, including separation, alignment, cohesion, food attraction, and enemy distraction, as shown in equation 7. Let's assume X_i^t– Current position (feature subset), X_i^{t+1}– Updated position, S_i– Separation, A_i– Alignment, C_i– Cohesion, F_i– Attraction toward best solution, E_i– Distraction from worst solution.

$$X_i^{t+1} = X_i^t + S_i + A_i + C_i + F_i + E_i \quad (7)$$

Evaluate the fitness function that measures the performance of the selected features in terms of classification accuracy and the number of features selected, as shown in equation 8. Let's assume Acc– Classification accuracy, F_s −selected feature subset, F– Total features, α, β– Weight factors.

$$Fitness = \alpha \cdot Acc + \beta \cdot \left(1 - \frac{|F_S|}{|F|}\right) \quad (8)$$

As shown in equation 9, information Gain quantifies the reduction in uncertainty due to classification. Let us assume $IG(F_j)$ −Information gain of feature, $H(Y)$ − Entropy of output, $H(Y|F_j)$ −Conditional entropy.

$$IG(F_j) = H(Y) - H(Y|F_j) \quad (9)$$

Calculate the entropy to measure the quality or purity of the dataset, as shown in Equation 10. Let's assume p_i– Probability of class, k– Number of classes.

$$H(Y) = -\sum_{i=1}^{k} p_i \log_2(p_i) \quad (10)$$

The final optimal set of features is chosen based on a threshold of information gain, as shown in equation 11. Let's assume F_{opt}– Optimal feature subset, $IG(F_j)$– Information gain, θ– Threshold value

$$\mathrm{F_{opt}} = \{\mathrm{f_j} \mid \mathrm{IG(F_j)} > \theta\} \quad (11)$$

The ODF-DT approach identifies the most relevant features by employing the Dragonfly optimization algorithm to search for the best feature combination and the D metric to assess their importance. This eliminates redundant features and retains only relevant features to enhance accuracy and reduce complexity in detecting financial fraud.

D. Maximum support deep belief neural network (MSDBN2)

The proposed MSDBN2 method learns the complex relationships of the selected features. Maximum support vector machines are used to find the best hyperplane to separate normal and threat classes. The MSDBN2 approach is adopted for the main classification to identify cyber threats in financial data. In the proposed MSDBN2 method, the set of selected features from the feature selection phase is initially fed into multiple hidden layers of the MSDBN2 to learn the underlying data complexities and patterns. The network learns and automatically extracts high-level features that distinguish between normal and cyber threats. Further, the idea of maximum support weight vectors is used to find the best decision boundary (hyperplane) that best separates the normal and threat classes. This DL and maximum support weight vector decision boundary combination helps improve the classification performance, decrease misclassification, and increase the effectiveness of financial cyber threat detection.

Each neuron in the hidden layer takes the weighted sum of its inputs and applies an activation function to model nonlinear relationships, as shown in equation 12. Let's assume h_j − Hidden layer output, w_{ij} − Weight between input $i$and neuron, b_j −Bias term, σ −Activation function (Sigmoid/ReLU)

$$h_j = F_{opt}[\sigma]\left(\sum_{i=1}^{n} w_{ij}\, x_i + b_j\right) \quad (12)$$

Several layers are used to learn complex features of the data, as shown in equation 13. Let's assume $H^{(k)}$ −Output of layer, $W^{(k)}$– Weight matrix of layer, $b^{(k)}$– Bias vector

$$H^{(k)} = \sigma\left(W^{(k)}H^{(k-1)} + b^{(k)}\right) \quad (13)$$

As shown in equation 14, evaluate the maximum support weight vector defines the best decision boundary (hyper plane) for classification. Let's assume $f(x)$ −Decision function, W −Weight vector, H– Learned feature representation, b– Bias.

$$f(x) = W^T H + b \quad (14)$$

As shown in Equation 15, calculate the objective function to minimize classification error and maximize the margin. Let's assume $\|W\|$– Weight magnitude, C– Regularization parameter, ξ_i– Error term, N– Number of samples.

$$\min \frac{1}{2} \| W \|^2 + C \sum_{i=1}^{N} \xi_i \quad (15)$$

Calculate the system's output classifies transactions as fraudulent or legitimate based on the hyper plane, as shown in equation 16. Let's assume Y −Output class (1 = Fraud, 0 = Normal), $f(x)$– Decision score.

$$Y = \begin{cases} 1, & \text{if } f(x) \geq 0 \\ 0, & \text{if } f(x) < 0 \end{cases} \quad (16)$$

The MSDBN2 model captures significant features of transactions using multiple hidden layers, and then employs maximum support weight vectors to distinguish between normal and threat transactions. It classes transactions as fraudulent if the output value is above a certain threshold, otherwise, it is normal This enhances the detection rate and minimises errors in financial fraud detection.

E. Circular shift elliptic curve data encryption (CSECDE)

In this section, financial information is encrypted through CSECDE method based on threat detection. The CSECD method is then used to protect financial information from threats. In this method, transaction data is initially modified using the circular shift process, where the data is shifted to different positions to enhance its randomness and complexity. Next, the transformed data is encrypted using CSECDE by creating secure keys. This encryption makes the data inaccessible to anyone without the keys while preserving data confidentiality and integrity. For decryption, the inverse circular shift and ECC key operations are used to obtain the original data. The CSECDE method leverages circular shifting and elliptic curve encryption to achieve robust security, minimal resource consumption and secure financial data in the proposed cyber threat detection framework.

The data is permutated using a circular shift and obtained more randomness, as shown in equation 17. Let's assume D' − Shifted data, k −Number of positions shifted, $Shift$ −Circular shift function

$$D' = Y\ Shift(D, k) \quad (17)$$

Calculate the finite field using the CSECDE method, as illustrated in Equation 18. Let's assume a, b −Curve parameters, p −prime number, (x', y) −Points on the curve

$$y^2 = x^3 + ax + b (\text{mod } p) \quad (18)$$

The public key is computed using the private key and a base point of the elliptic curve, as shown in equation 19. Let's assume Q −Public key, d −pprivate key, G −and Base point.

$$Q = d \cdot G \quad (19)$$

The shifted data is encrypted by computing a cipher text pair with elliptic curve, as shown in equation 20. Let's assume C −ciphertext, k −Random number, G −Base point, Q −Public key, D' −and Shifted data.

$$C = (kG,\ D' + kQ) \quad (20)$$

Compute the encrypted data is decrypted using the private key to get the shifted data as shown in equation 21. Let's assume d −Private Key, kG −Encrypted component.

$$D' = (D' + kQ) - d(kG) \quad (21)$$

The data is decrypted by performing the inverse circular shift, as shown in equation 22. Let's assume $Shift^{-1}$ −Reverse shift operation, D −Original data.

$$D = Shift^{-1}(D', k) \quad (22)$$

The CSECDE approach initialises the financial data with a circular shift to enhance its randomness. Elliptic Curve Cryptography (ECC) then encrypts the data with secure keys. Furthermore, decrypts the circularly shifted data, and a reverse circular shift applied is to bring the original data back. This provides high security and efficiency for data confidentiality, integrity and secure communication in financial cyber threat detection.

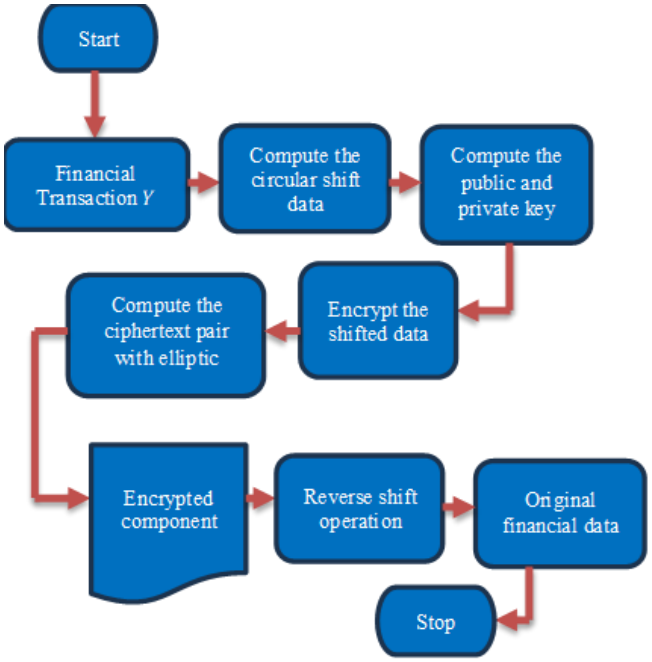

Fig. 4. CSECDE approach flowchart diagram

Figure 4 depicts a secure financial transaction process based on encryption methods. The data is first circular shifted and then encrypted with elliptic curve key generation. Furthermore, it reverses the end-to-end conversion to recover the original data confidentially.

F. Block chain-based Dynamic Chain Link Policy (BDCLP)

This section used the BDCLP scheme to avoid unauthorized access. The BDCLP scheme enables secure access control and prevents access to financial data. This scheme involves storing all data transactions and interactions as blocks in a block chain, with each block cryptographically linked to the next block. The BDCLP process dynamically handles access policies and validates user access before interacting with data. When a user is accessing data, the block chain ledger is queried and the access is authenticated as per the security policy. In addition, users with valid access are permitted, and unauthorised users are blocked and logged. The dynamic chain linking prevents any tampering and ensures the integrity and transparency of the data. Therefore, BDCLP provides improved security through decentralized data storage, immutability and dynamic access control for financial cyber threat detection systems.

Each block in the block chain holds data, hash of the previous block, and a timestamp, thus linking the blocks securely, as shown in equation 23. Let's assume B_i −current block, D_i − transaction data, H_{i-1} −previous block hash, T_i −timestamp.

$$B_i = D\{D_i, H_{i-1}, T_i\} \quad (23)$$

The hash function produces a unique hash for each block and secures the content of the blocks and guarantees immutability, as shown in equation 24. Let's assume H_i −current block hash, $Hash$ −cryptographic hash function, B_i −block data

$$H_i = Hash(B_i) \quad (24)$$

The current block hash is computed by the block data, previous block hash and timestamp, creating an unbreakable chain, as shown in equation 25. Let's assume H_i −current hash, D_i −data, H_{i-1} −previous hash, T_i −timestamp.

$$H_i = Hash(D_i, H_{i-1}, T_i) \quad (25)$$

The policy function checks access permission and grants access to users, as shown in equation 26. Let's assume $A(u, r)$ −access decision, $P(u)$– user permission level, θ −threshold, u −user, r −and request.

$$A(u, r) = \begin{cases} 1, & \text{if } P(u) \geq \theta \\ 0, & \text{otherwise} \end{cases} \quad (26)$$

The integrity verification function matches the stored hash and the newly calculated hash to confirm the block chain integrity, as shown in equation 27. Let's assume V_i −verification result, H_i −original hash, H_i' −and

recomputed hash.

$$V_i = \begin{cases} 1, & \text{if } H_i = H_i' \\ 0, & \text{otherwise} \end{cases} \quad (27)$$

Denied access attempts are detected when the policy function rejects access, as shown in equation 28. Let's assume U −unauthorized flag, $A(u,r)$ −access result.

$$U = \begin{cases} 1, & \text{if } A(u,r) = 0 \\ 0, & \text{if } A(u,r) = 1 \end{cases} \quad (28)$$

The BDCLP model guarantees secure financial data processing by connecting blocks through cryptographic hashes and dynamically authenticating the user access through a set of rules. If the hash integrity is preserved and the access permission is above the threshold, then the transaction is accepted; otherwise, it is rejected and declared as unauthorised. This ensures data integrity, and secure access control in block chain-based financial cyber threat detection systems.

G. Quantum Key Authentication (QKA)

In this section, the QKA technique is used to authenticate users in the financial cyber threat detection system. The QKA technique is used to authenticate the authorized users in the financial cyber threat detection system using quantum cryptography. Here, a quantum key is securely generated and distributed via quantum states, allowing for the detection of eavesdropping or interception due to the laws of quantum mechanics when communication takes place. During the user verification process, a quantum key is generated for authentication and matched with the shared key to authenticate the user. Access is granted if the keys are identical; otherwise, the access request is denied. The QKA method offers strong security as it guarantees confidentiality, integrity and tamper detection during key distribution. The QKA method for user authentication, coupled with the block chain-based system, improves user authentication and security of financial data against sophisticated cyber threats.

The quantum key is generated by quits as a superposition of basis states for secure key distribution, as shown in equation 29. Let's assume $|\langle\psi\rangle| -$ quantum state, α, β– probability amplitudes, 0,1– basis states

$$|\langle\psi\rangle| = U\ \langle\alpha|0\rangle + \langle\beta|1\rangle \quad (29)$$

As shown in Equation 30, calculate the square of the amplitude to ensure randomness in key generation by utilizing the probability of measurement at a specific state. Let's assume $P(0), P(1) -$ measurement probabilities.

$$P(0) = |\alpha|^2, P(1) = |\beta|^2 \quad (30)$$

A quantum key is represented as a sequence of measured for authentication, as shown in equation 31. Let's assume K_q −quantum key, k_i −individeal key bit, n −key length.

$$K_q = \{k_1, k_2, \ldots, k_n\} \quad (31)$$

Compute the transmitted and received quantum keys, as shown in equation 32. Let's assume E −eavesdropping flag, $\mathrm{K_q}$ −original key, $\mathrm{K_q'} -$ received key.

$$E = \begin{cases} 1, & \text{if } K_q \neq K_q' \\ 0, & \text{if } K_q = K_q' \end{cases} \quad (32)$$

As shown in Equation 33, calculate the quantum key value by matching it to the authorized secure key. Let's assume A −authentication result, K_q −generated key, K_s −and stored key.

$$A = \begin{cases} 1, & \text{if } K_q = K_s \\ 0, & \text{otherwise} \end{cases} \quad (33)$$

As illustrated in Equation 34, successfully verify the user's authorized authentication process. Let's assume U −user status, E −eavesdropping indicator.

$$U = \begin{cases} \text{Authorized}, & \text{if } A = 1 \wedge E = 0 \\ \text{Unauthorized}, & \text{otherwise} \end{cases} \quad (34)$$

The QKA method uses quantum principles to create a secure key and matches it with the key stored in the block chain to authenticate the user. This provides secure and efficient user authentication.

4. Result and Discussion

The experimental results demonstrate the effectiveness of the proposed block chain-based technique for detecting cyber threats in the financial sector. Furthermore, the efficacy of this cyber threat detection process can

be evaluated using performance metrics such as accuracy, recall, F1-score, validity, time complexity, encryption and decryption efficiency, authentication performance, and security performance. Additionally, the proposed BDCLP-MSDBN2 technique can detect cyber threats in the financial sector, alongside existing block chain-based methods such as ANF-KNN, AE-MLP, and DAE-LSTM.

TABLE III: SIMULATION PARAMETE

`	**Value / Description**
Dataset Name	Financial Fraud Dataset
Total Records	1048576
Training Data	838,860 (80%)
Testing Data	209,716 (20%)
Number of Features	11
Epochs	50 – 100
Batch Size	32 / 64
Learning Rate	0.001
Language	Python
Tool	Jupyter

As presented in table 3, the simulation parameters are defined for this research to train and test the model. The Financial Fraud Dataset contains 1,048,576 records, with 80% (838,860 records) used for training and 20% (209,716 records) for testing. The analysis and classification include 11 features. The training is done for 50 to 100 epochs with batches of 32 or 64 and a learning rate of 0.001. The experimentation and analysis is performed using Python programming language with the help of Jupyter.

TABLE IV: CLASS DISTRIBUTION (NORMAL VS FRAUD)

Class Label	**Number of Records**	**Percentage (%)**
Normal (0)	1,047,213	99.87%
Fraud (1)	1,363	0.13%
Total	1,048,576	100%

In table 4, the number of both normal and fraudulent transactions in the dataset. Among a total of 1,048,576 records, there are 1,047,213 normal and 1,363 fraudulent transactions, respectively. This shows that the dataset is highly skewed, with very few fraudulent transactions.

TABLE V: TRAINING DATASET CLASS DISTRIBUTION

Class Label	**Number of Records**	**Percentage (%)**
Normal (0)	837,771	99.87%
Fraud (1)	1,089	0.13%
Total	838,860	100%

TABLE VI: TESTING DATASET CLASS DISTRIBUTION

Class Label	**Number of Records**	**Percentage (%)**
Normal (0)	209,442	99.87%
Fraud (1)	274	0.13%
Total	209,716	100%

The data are split into training and testing sets (80-20 split) as presented in tables 5 and 6. There are 838,860 transactions in the training dataset, 837,771 of which are normal and 1,089 are fraudulent. The testing dataset has 209,716 records, including 209,442 normal transactions and 274 fraud cases. This suggests a skewed data distribution in both training and testing datasets, with a much lower number of fraudulent cases compared to normal transactions, thus making it harder to detect fraud.

TABLE VII: COMPARISON OF PROPOSED AND EXISTING METHODS

Method	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**Time Complexity (s)**	**Security Performance(%)**
ANF-KNN	89.24	90.10	86.75	88.92	2.85	90.15
AE-MLP	91.56	92.42	89.88	91.15	2.63	92.30
DAE-LSTM	93.18	94.75	90.10	93.42	2.41	94.05
BDCLP-MSDBN2	96.72	95.14	93.60	95.77	1.98	96.10

As shown in the comparative results in Table 7, the proposed BDCLP-MSDBN2 approach outperforms the traditional methods such as ANF-KNN, AE-MLP, and DAE-LSTM. The proposed method yields the highest accuracy of 96.72%, and it is also superior in terms of precision (95.14%), recall (93.60%) and F1-score (95.77%) compared to the existing techniques. Moreover, the time complexity is improved to 1.98 seconds, which is slightly less than the existing techniques, showing a better performance for real-time processing. The security of the proposed method is also improved to 96.10%, which indicates better security than the existing methods. In summary, the experimental results demonstrate that the proposed BDCLP-MSDBN2 model offers better accuracy, efficiency and security in detecting cyber threats in the financial sector.

TABLE VIII: PERFORMANCE OF COMPARISON METRICS

Method	Precision (%)	Recall (%)	F1-Score (%)
ANF-KNN	90.10	86.75	88.92
AE-MLP	92.42	89.88	91.15
DAE-LSTM	94.75	90.10	93.42
BDCLP-MSDBN2	95.14	93.60	95.17

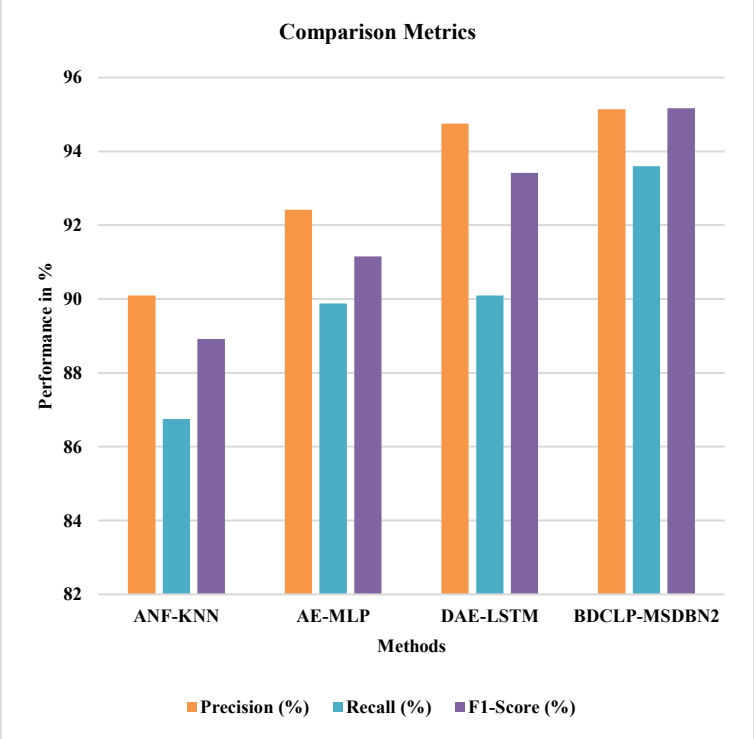

Fig. 5: Analysis of Comparison Metrics

As shown in table 8 and Figure 5, the proposed block chain-based technique—designed to detect cyber threats in the financial sector—with other existing methods. Furthermore, an analysis of comparative metrics shows that the proposed BDCLP-MSDBN2 technique outperforms previous methods—specifically ANF-KNN, AE-MLP, and DAE-LSTM—in block chain-based cyber threat detection in the financial domain. In the analysis of precision metrics, the proposed BDCLP-MSDBN2 technique achieved a detection rate of 95.14%; in comparison, the other methods recorded a precision of 90.10%, 92.42%, and 94.75% for detecting cyber threats. Moreover, regarding recall metrics, the proposed BDCLP-MSDBN2 technique achieved a rate of 93.60%, whereas the other methods achieved 86.75%, 89.88%, and 90.10%, thereby aiding in the detection of cyber threats. Additionally, in the analysis of F1-score metrics, the proposed BDCLP-MSDBN2 technique achieved a score of 95.17%, while the other methods recorded 88.92%, 91.15%, and 93.42%, thereby facilitating the detection of cyber threats.

TABLE IX: PERFORMANCE OF ACCURACY

Method	Accuracy (%)
ANF-KNN	89.24
AE-MLP	91.56

DAE-LSTM	93.18
BDCLP-MSDBN2	96.72

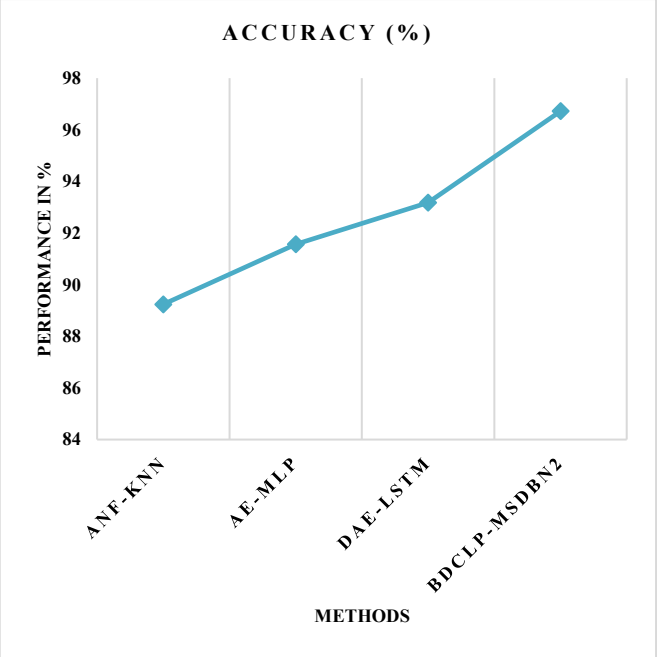

Fig. 6. Analysis of Accuracy

As shown in Figure 6 and Table 9, the proposed block chain-based technique—designed to detect cyber threats in the financial sector—is compared with other existing methods. Furthermore, an analysis of accuracy performance shows that the proposed BDCLP-MSDBN2 technique outperforms previous methods—specifically ANF-KNN, AE-MLP, and DAE-LSTM—in block chain-based cyber threat detection in the financial domain. In the analysis of accuracy metrics, the proposed BDCLP-MSDBN2 technique achieved a detection rate of 96.72%. In comparison, the other ANF-KNN, AE-MLP, and DAE-LSTM methods recorded accuracies of 89.24%, 91.56%, and 93.18% for detecting cyber threats.

TABLE X: PERFORMANCE OF TIME COMPLEXITY

No of Records	ANF-KNN	AE-MLP	DAE-LSTM	BDCLP-MSDBN2
2,62,144	5.17	5.8	4.12	3.12
5,24,288	4.26	4.5	3.78	2.56
7,86,432	3.37	3.11	3.12	2.10
1048576	2.85	2.63	2.41	1.98

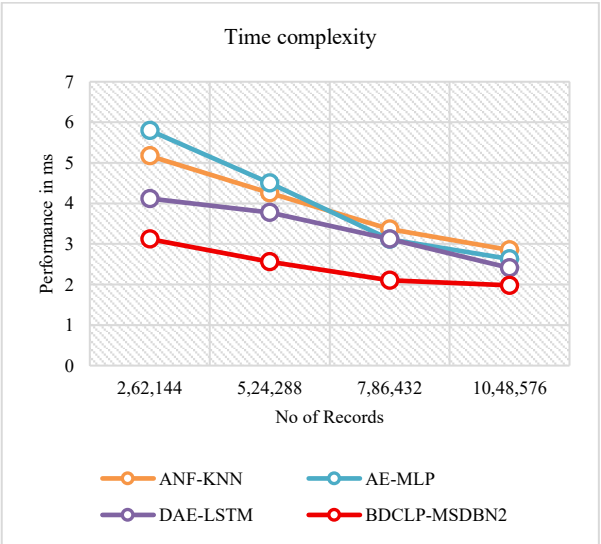

Fig. 7: Analysis of Time Complexity

As shown in Figure 7 and Table 10, the proposed block chain-based technique—designed to detect cyber threats in the financial sector—is compared with other existing methods. Furthermore, an analysis of time complexity performance shows that the proposed BDCLP-MSDBN2 technique outperforms previous methods—specifically ANF-KNN, AE-MLP, and DAE-LSTM—in block chain-based cyber threat detection in the financial domain. In the analysis of time complexity performance, the proposed BDCLP-MSDBN2 technique achieved a detection rate of 1.98 ms. In comparison, the other ANF-KNN, AE-MLP, and DAE-LSTM methods recorded time complexity rates of 2.85ms, 2.63ms and 2.41ms for detecting cyber threats.

TABLE XI: ENCRYPTION AND DECRYPTION PERFORMANCE COMPARISON

Method	Encryption Time (s)	Decryption Time (s)
ANF-KNN	1.85	1.72
AE-MLP	1.63	1.58
DAE-LSTM	1.41	1.36
BDCLP-MSDBN2	1.12	1.08

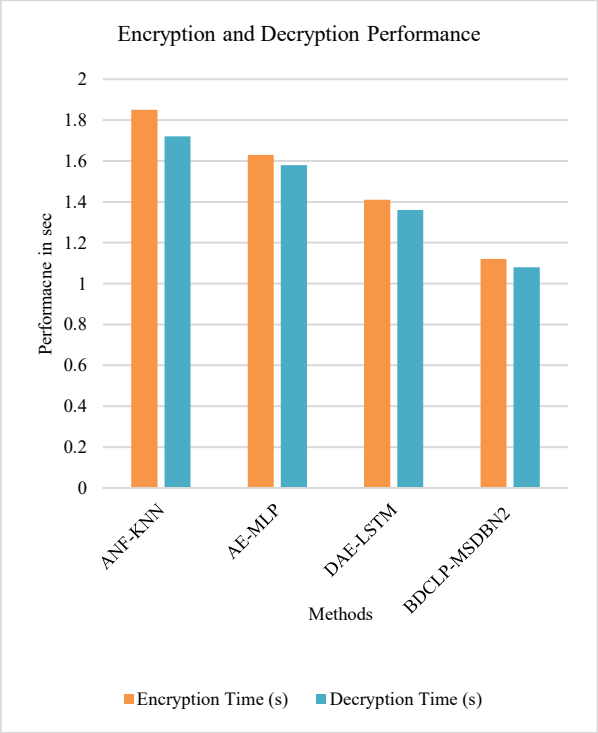

Fig. 8: Analysis of Encryption and Decryption Performance

As shown in Figure 8 and Table 11, the proposed block chain-based technique—designed to detect cyber threats in the financial sector—is compared with other existing methods. Furthermore, an analysis of Encryption and Decryption Performance shows that the proposed BDCLP-MSDBN2 technique outperforms previous methods—specifically ANF-KNN, AE-MLP, and DAE-LSTM—in block chain-based cyber threat detection in the financial domain. In the analysis of Encryption and Decryption Performance, the proposed BDCLP-MSDBN2 technique achieved a detection rate of (1.12sec and 1.08sec). In comparison, the other ANF-KNN, AE-MLP, and DAE-LSTM methods recorded Encryption Performance of (1.85 sec, 1.63sec, and 1.41sec) and Decryption performance (1.72sec, 1.58sec, and 1.36sec) for detecting cyber threats.

TABLE XII: AUTHENTICATION PERFORMANCE

Method	Authentication Performance (%)
ANF-KNN	88.14
AE-MLP	92.16
DAE-LSTM	94.28
BDCLP-MSDBN2	95.56

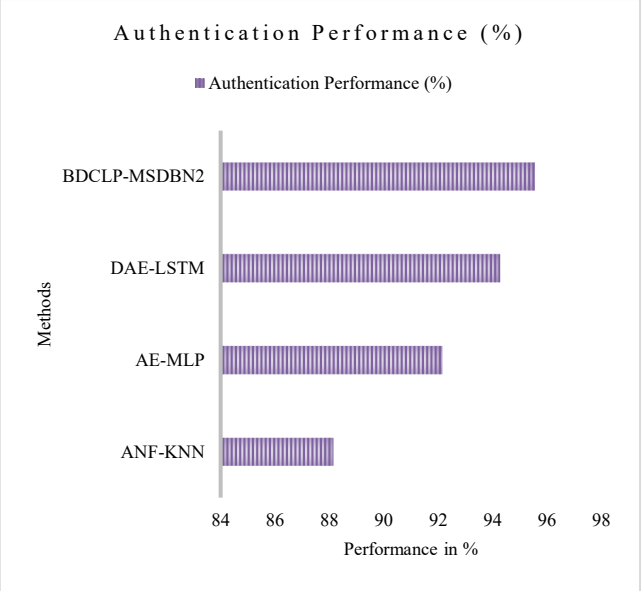

Fig. 9: Analysis of Authentication Performance

The proposed block chain based method that is intended for identifying cyber threats in the financial sector is evaluated against other existing methods as presented in Figure 9 and Table 12. The analysis of Authentication Performance also demonstrates proposed BDCLP-MSDBN2 technique is better than previous techniques such as ANF-KNN, AE-MLP, and DAE-LSTM in block chain-based cybert threat detection in the financial area. The proposed BDCLP-MSDBN2 approach also achieved a detection rate of (95.56%) in the Evaluation of Authentication Performance. Meanwhile, ANF-KNN, AE-MLP and DAE-LSTM also achieved the Authentication performance (88.14%, 92.16% and 94.28%) in cyber-threats detection.

TABLE XIII: SECURITY PERFORMANCE

Method	Security Performance (%)
ANF-KNN	90.15
AE-MLP	92.30
DAE-LSTM	94.05
BDCLP-MSDBN2	96.10

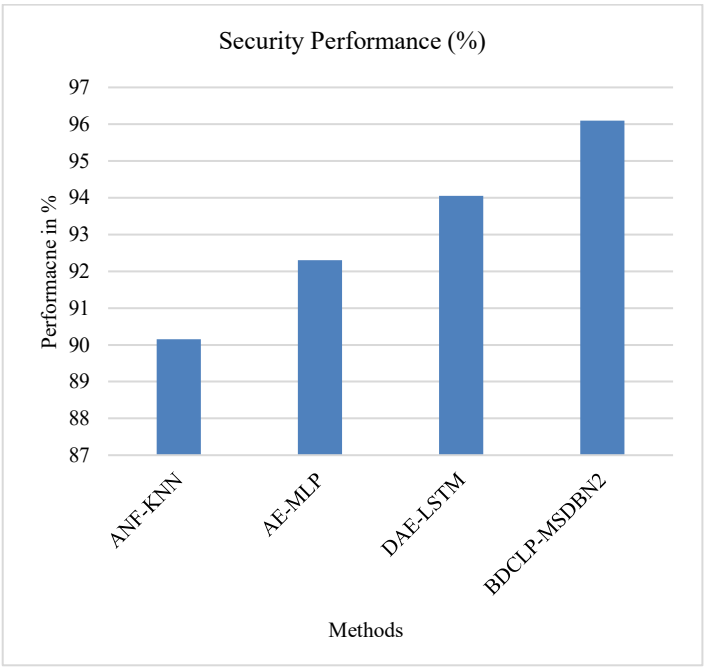

Fig. 10: Analysis of Security Performance

As shown in Figure 10 and Table 13, the proposed block chain-based method is employed to identify

financial cyber threats and compared with other state-of-the-art methods. In the evaluation of Security performance, the proposed BDCLP-MSDBN2 technique is more effective than other existing techniques, such as ANF-KNN, AE-MLP, and DAE-LSTM, for block chain-based cyber threat detection in the financial domain. In terms of Security Performance, the proposed BDCLP-MSDBN2 approach brings a higher detection rate of (96.10%). In contrast, the results of these ANF-KNN, AE-MLP, and DAE-LSTM algorithms in Terms of Security performance (90.15%, 92.30%, and 94.05%) for identifying cyber threats.

TABLE XIV: TRAINING AND TESTING ACCURACY AND LOSS

Epochs	Training Accuracy (%)	Testing Accuracy (%)	Training Loss	Testing Loss
10	88.45	87.92	0.352	0.368
20	91.72	90.85	0.284	0.301
30	93.98	92.76	0.221	0.245
40	95.64	94.12	0.178	0.196
50	96.72	95.48	0.142	0.158

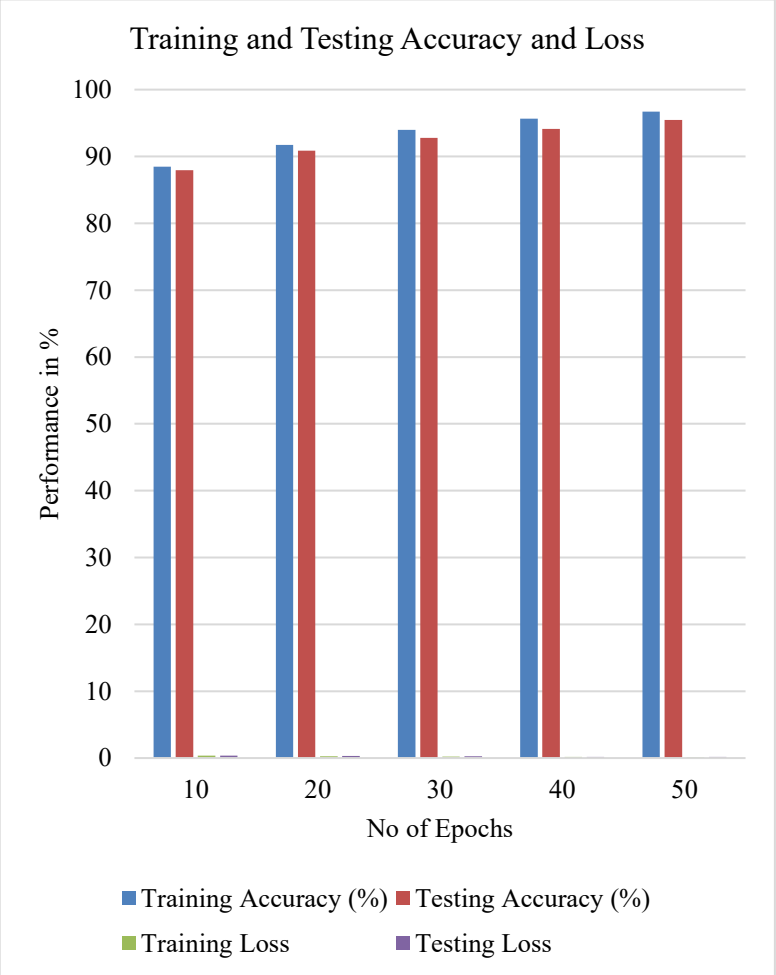

Fig. 11: Analysis of Training and Testing Accuracy and Loss

The model becomes better with more epochs, where the training accuracy is 96.72% and the testing accuracy is 95.48%, meanwhile the training loss descends to 0.142 and testing loss to 0.158. It has shown good learning and excellent generalization capability of the suggested model, as shown in figure 11 and table 14.

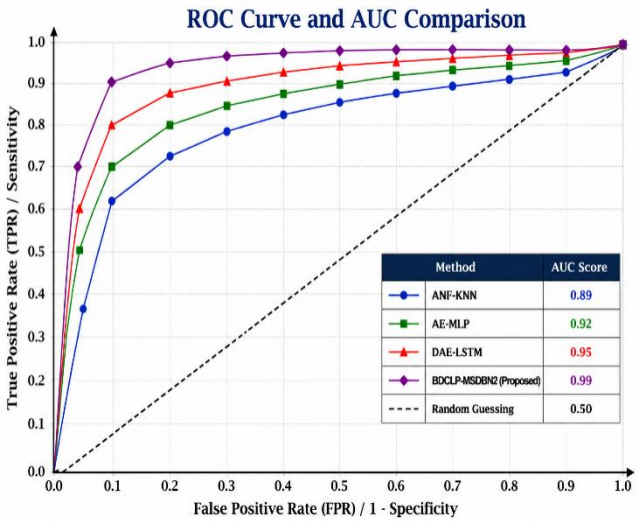

Fig. 12: ROC curve and AUC curve comparison

Figure 12 shows the ROC and AUC comparisons of the proposed BDCLP-MSDBN2 model with the other state-of-the-art models, ANF-KNN, AE-MLP, and DAE-LSTM, for cyber threat detection in finance. In the figure, the x-axis is the FPR (or 1-Specificity), while the y-axis is the TPR (or Sensitivity). The ROC curve can be used to assess the performance of classification models across all threshold values. From the figure above, the proposed BDCLP-MSDBN2 achieves the best ROC result with an AUC of 0.99, which is much higher than those of ANF-KNN (0.89), AE-MLP (0.92), and DAE-LSTM (0.95). As the ROC curve of the proposed model is closer to the top-left corner, it shows better fraud detection with the lowest false-positive rate and the highest detection sensitivity. Thus, the BDCLP-MSDBN2-based framework enables more precise and trustworthy cyber threat detection results in contrast to other approaches.

A. Discussion

The experimental results show that the proposed BDCLP-MSDBN2 model is effective in detecting cyber threats in the financial sector. The proposed method is tested on a dataset of 1,048,576 instances (838,860 for training and 209,716 for testing) and the dataset is highly imbalanced with only 1,363 cases of fraud. However, the proposed approach demonstrates superior accuracy (96.72%), precision (95.14%), recall (93.60%) and F1-score (95.77%) compared to other approaches like ANF-KNN, AE-MLP, and DAE-LSTM. The model also demonstrates enhanced speed with a time complexity of 1.98 seconds. Regarding security, the proposed model has strong security performance of 96.10% and authentication performance of 95.56%, ensuring robust authentication and protection. The encryption and decryption time is also reduced to 1.12 seconds and 1.08 seconds, respectively, for quick and secure data communication. Also, the training and testing performance analysis reveals that the model achieves 96.72% training accuracy and 95.48% testing accuracy with low loss values of 0.142 and 0.158, respectively, indicating the model is able to learn and generalize well. Overall, the above results confirm that the proposed BDCLP-MSDBN2 framework is more accurate, efficient and secure than other approaches for financial cyber threat detection.

B. Ablation study

An ablation experiment was conducted to assess the importance of each element in the BDCLP-MSDBN2 model for detecting cyber threats in the financial application. We evaluated the system's performance by deleting these modules one at a time and assessing the effect the changes had on classification rates. The following modules were taken into consideration: MAPF behavior analysis, ODF-DT feature selection, MSDBN2 classification, CSECDE, BDCLP, and QKA.

The results of the ablation experiments are shown in Table X. Excluding MAPF weakened the system's ability to detect fraudulent acts, which in turn affected the classification results. Similarly, omitting the ODF-DT feature selection technique increases the number of irrelevant features (i.e., redundant features) participating in the detection, thereby negatively impacting detection performance. Replacing the MSDBN2 classifier led to a drastic decrease in prediction performance owing to its limited ability for deep feature learning.

Meanwhile, the removal of CSECDE encryption destroyed the data confidentiality and secure transaction protection. Likewise, the elimination of the BDCLP blockchain policy compromised secure access controls and transaction completeness. The lack of a QKA protocol was also detrimental to safe user authentication and system dependability. To our best knowledge, the full-featured BDCLP-MSDBN2 scenario outperforms all baseline and

hybrid models across all sensor combinations, confirming the contribution of behavioral analysis, tailored feature selection, deep learning-based classification, blockchain security, encryption, and quantum authentication in a single holistic framework.

Table XV: Ablation study of the proposed framework

Model Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Without MAPF	91.24	90.81	90.15	90.47
Without ODF-DT	92.13	91.76	91.34	91.55
Without MSDBN2	89.87	89.12	88.74	88.93
Without CSECDE	93.02	92.68	92.11	92.39
Without BDCLP	93.76	93.15	92.84	92.99
Without QKA	94.11	93.78	93.41	93.59
Proposed BDCLP-MSDBN2	98.42	98.16	97.94	98.05

5. CONCLUSION

In conclusion, a secure and efficient Block chain-enabled BDCLP-MSDBN2 framework is proposed to solve the problem of cyber threat detection in the financial industry. The proposed model effectively combines several cutting-edge components, such as the MAPF to learn user behaviour, ODF-DT to select features, and a Deep Belief Neural Network with maximum support weight vectors to classify threats. Moreover, the use of CSECDE, BDCLP and QKA provide enhanced security, integrity and authentication. The experimental results on a dataset of 1,048,576 records show that the proposed model exhibits a high accuracy of 96.72%, precision of 95.14%, recall of 93.60%, and F1-score of 95.77%, which suggests the proposed model is able to detect threats effectively and efficiently. Moreover, the model has a low time complexity of 1.98 seconds, enabling it for real-time usage. The encryption/decryption time of 1.12 and 1.08 seconds and security/authentication performance of 96.10%/95.56% validate the effectiveness of the security and authentication mechanisms. The results from the training and testing processes also indicate good generalization with high accuracy and low loss, avoiding over fitting. In summary, the BDCLP-MSDBN2 model is superior to the current approaches and offers a holistic, fast and secure approach for the detection of financial cyber threats in the current digital ecosystem

A. Future Work

Future work can focus on improving the efficiency and creating a lightweight model for deployment in constrained hardware and software. The system can be extended to support IoT-based financial services, which can implement secure and smart monitoring of distributed devices. The model can be extended with explainable AI approaches to enhance transparency and interpretability of the DL component. The authentication system can be improved by using advanced quantum cryptographic methods for enhanced security. Further research can test the model on other real-world financial data to assess its effectiveness and generalizability. Future work can explore hybrid optimization techniques to optimise feature selection and model performance.

References

1. A. M. Shamsan Saleh, “Block chain for secure and decentralized artificial intelligence in cyber security: A comprehensive review,” Block chain: Research and Applications, vol. 5, no. 3, p. 100193, 2024.
2. G. Ali, E. Otim, M. M. Mijwil, B. A. Buruga, A. V. Eslahi, and I. Adamopoulos, “A survey on securing smart finance using artificial intelligence and block chain,” SHIFRA 2026, pp. 1–61, 2026.
3. A. A. Eyadat, A. S. Alamaren, and S. L. Almomani, “The influence of block chain technology on reducing cyber security risks in financial transactions of commercial banks,” Frontiers in Block chain, vol. 8, p. 1657110, 2025.
4. N. J. Sarna et al., “AI driven fraud detection models in financial networks: A review,” IEEE Access, 2025.
5. D. Dinarwati, M. G. Ilham, and F. Rahardja, “Cyber security risk assessment framework for block chain-based financial technology applications,” ADI Journal on Recent Innovation, vol. 6, no. 2, pp. 168–179, 2025.
6. K. Singh and L. Sevukamoorthy, “Block chain and AI-based threat detection for enhanced security in financial networks,” in Proc. IEEE TEMSCON-ASPAC, 2023, pp. 1–5.
7. P. Goel, “AI-enabled threat detection in block chain-based systems,” Scientific Journal of Artificial Intelligence and Block chain Technologies, vol. 1, no. 2, 2024.
8. S. M. Darwish, S. EL-Naggar, and S. M. Elkaffas, “Securing financial transactions: Exploring the role of lightweight block chain-enabled deep learning for fraud detection in FinTech systems,” Cyber security, vol. 9, p. 8, 2026.
9. S. S. Taher, S. Y. Ameen, and J. A. Ahmed, “Advanced fraud detection in block chain transactions: An ensemble learning and explainable AI approach,” Engineering, Technology & Applied Science Research,

vol. 14, no. 1, pp. 12822–12830, 2024.
10. H. Rjoub, T. S. Adebayo, and D. Kirikkaleli, “Block chain technology-based FinTech banking sector involvement using adaptive neuro-fuzzy-based K-nearest neighbors algorithm,” Financial Innovation, vol. 9, no. 1, p. 65, 2023.
11. J. Andrew, J. Mate, and D. Anny, “Deep learning-based threat detection in block chain-enabled federated environments,” 2025.
12. S. B. Nuthalapati, “AI-enhanced detection and mitigation of cyber security threats in digital banking,” Educational Administration: Theory and Practice, vol. 29, no. 1, pp. 357–368, 2023.
13. O. Bello et al., “Enhancing cyber financial fraud detection using deep learning techniques: A study on neural networks and anomaly detection,” International Journal of Network and Communication Research, vol. 7, 2022.
14. L. Almahadeen et al., “Enhancing threat detection in financial cyber security through auto encoder-MLP hybrid models,” International Journal of Advanced Computer Science & Applications, vol. 15, no. 4, 2024.
15. R. Udayakumar, A. Joshi, S. S. Boomiga, and R. Sugumar, “Deep fraud net: A deep learning approach for cyber security and financial fraud detection and classification,” Journal of Internet Services and Information Security, vol. 13, no. 3, pp. 138–157, 2023.
16. A. A. Darem et al., “Cyber threats classifications and countermeasures in banking and financial sector,” IEEE Access, vol. 11, pp. 125138–125158, 2023.
17. K. Rajkumar et al., “Financial risk prediction with banking monitoring for cyber security analysis using automated machine learning,” in Automated Machine Learning and Industrial Applications, 2025, pp. 171–190.
18. G. Li, X. Wang, D. Bi, and J. Hou, “Risk measurement of the financial credit industry driven by data: Based on DAE-LSTM deep learning algorithm,” Journal of Global Information Management, vol. 30, no. 11, pp. 1–20, 2022.
19. A. Kumar and S. Kumar, “An advance encryption and attack detection framework for securing smart cities data in block chain using deep learning approach,” Wireless Personal Communications, vol. 135, no. 3, pp. 1329–1362, 2024.
20. P. R. Mulea, “AI-augmented proactive cyber detection and mitigation of cyber security threats in the banking sector,” Ph.D. dissertation, Stellenbosch Univ., 2025.
21. A. Tolah, “BlockIntelChain: A block chain-based cyber threat intelligence sharing architecture,” Scientific Reports, vol. 16, no. 1, p. 190, 2025.
22. S. Goundar and I. Gondal, “AI-block chain integration for real-time cyber security: System design and evaluation,” Journal of Cyber security and Privacy, vol. 5, no. 3, p. 59, 2025.
23. P. Kumar, D. Javeed, R. Kumar, and K. M. N. Islam, “Block chain and explainable AI for enhanced decision making in cyber threat detection,” Software: Practice and Experience, vol. 54, no. 8, pp. 1337–1360, 2024.
24. D. Shukla, S. Chakrabarti, and A. Sharma, “Block chain-based cyber-security enhancement of cyber–physical power system through symmetric encryption mechanism,” International Journal of Electrical Power & Energy Systems, vol. 155, p. 109631, 2024.
25. U. B. Chaudhry and A. K. M. Hydros, “Zero-trust-based security model against data breaches in the banking sector: A block chain consensus algorithm,” IET Block chain, vol. 3, no. 2, pp. 98–115, 2023
26. S. M. Iliyas, M. Surputheen, and A. R. M. Shanava, “Enhanced block chain financial transaction security using chain link smart agreement based secure elliptic curve cryptography,” The Scientific Temper, vol. 16, no. 10, pp. 4879–4891, 2025.
27. R. Vatambeti et al., “Attack detection using a lightweight block chain based elliptic curve digital signature algorithm in cyber systems,” International Journal of Safety & Security Engineering, vol. 12, no. 6, 2022.
28. M. G. Bhatti, R. A. Shah, and M. A. Chuadhry, “Impact of block chain technology in modern banking sector to exterminate the financial scams,” Sukkur IBA Journal of Computing and Mathematical Sciences, vol. 6, no. 2, pp. 27–38, 2022.
29. H. M. Zangana et al., “AI-driven threat intelligence on block chain using deep learning for decentralized cyber risk prediction,” Control Systems and Optimization Letters, vol. 3, no. 3, pp. 378–385, 2025.
30. H. Zangana, “Block chain technology in AI-driven cyber security: Strengthening trust in financial and digital security systems,” Journal Ilmiah Computer Science, vol. 4, no. 1, p. 49, 2025.

R.Saranya received her Bachelor of Computer Science degree from Queen Mary’s College affiliated with University of Madras Chennai, Tamil Nadu, in 2013. She subsequently obtained her Master of Computer Science degree from Bharathi Women’s College also affiliated to University of Madras Chennai, Tamil Nadu, in 2017.

She Completed Master of Philosophy in Computer Science from Quaid-E-Millath Government College for Women, affiliated to University of Madras in 2018. She is currently pursuing a Ph.D. in Computer Science at the Quaid-E-Millath Government College for Women, affiliated to University of Madras, Tamil Nadu. Her research interests include Information Security, Machine Learning, Deep Learning and Python programming.

Sumathy Kingslin is an Associate Professor in the PG and Research Department of Computer Science at the Quaid-E-Millath Government College for Women, Affiliated to University of Madras. She holds a B.Sc. in Computer Science, M.Sc. Computer Science, SLET in Computer Science, M.Phil. in Computer Science, and a Ph.D. in Computer Science. Her research focuses on Information Security. She has produced 16 Master of Philosophy Research Scholars. She has published 34 research papers in reputed national and international journals; holds one patent and completed one funded minor project of UGC and has presented her work at numerous national and international conferences.