



# Blockchain-Enabled AI-Driven Fraud Detection System in Digital Banking

<sup>1</sup>Karthik Kushala

*Taylor Corporation, Minnesota, USA*  
karthik.kushala@gmail.com

<sup>2</sup>Vijai Anand Ramar

*Delta Dental Insurance Company, Georgia, USA*  
vijaianandramar@gmail.com

<sup>3</sup>Priyadarshini Radhakrishnan

*IBM Corporation, Ohio, USA*  
priyadarshinir990@gmail.com

<sup>4</sup>Yashwant Kumar Kolli

*Cognizant Technology Solutions US Corp, College Station, Texas, USA*  
yashkolli04@gmail.com

<sup>5</sup>Venkataramesh Induru

*Piorion Solutions Inc, New York, USA*  
venkatarameshinduru@gmail.com

<sup>6</sup>Thanjaivadivel M

*Nandha Engineering College, Erode, Tamil Nadu 638052, India*  
thanjaivadivelm@gmail.com

## Abstract

As online banking advances rapidly, securing digital platforms from complex fraud and privacy risks is growing ever more demanding. Conventional security approaches fail in cloud environments quite frequently. In this paper, a sound framework using blockchain technology and cloud computing is presented for augmenting security, transparency, and integrity of data in digital banking. The decentralized, tamper-evident characteristics of blockchain make its transaction history auditable and tamper-proof. Supporting this, a new hybrid deep learning (DL) framework Autoencoder (AE)-Long Short-Term Memory (LSTM)-Attention Mechanism (ATTM) is presented for smart fraud detection. The model integrates Autoencoders to extract features, LSTM networks to capture transaction patterns, and an Attention Mechanism to identify major fraud-related indicators. Tested using traditional metrics, the model performs a maximum accuracy of 96.2%, remarkably outperforming traditional machine learning algorithms such as Logistic Regression (LR), SVM, and Random Forest (RF). It also performs well in identifying infrequent fraud

instances while keeping false positives to a minimum. This research proves that combining blockchain with DL in a cloud setting provides a secure, scalable, and reliable solution for next-generation digital banking systems.

**Keywords:** Blockchain, Cloud Computing, Digital Banking Security, AE-LSTM-ATTM Hybrid Model, Fraud Detection, Deep Learning, Attention Mechanism.

## I. Introduction

The emergence of digital banking has revolutionized the banking sector by offering quick, convenient, and accessible services at anytime and anywhere. Transactions, account management, and financial products can be operated through digital platforms, which are now being deployed on cloud infrastructure for better scalability and operational performance [1]. Yet, this digitalization is accompanied by increasing fears over data security, privacy, cyberattacks, regulation compliance, and customer confidence [2]. As cyberattacks become more sophisticated and persistent, conventional



cloud security models are challenged to safeguard the sensitive financial information processed and stored by digital banking systems [3]. Blockchain technology has come forward as a revolutionary result to all of these issues [4]. Being characterized by decentralization, transparency, immutability, and advanced cryptographic security, blockchain can immensely enhance the security of digital banking services when combined with cloud platforms [5]. A cloud infrastructure based on blockchain makes it possible that records of transactions are safely duplicated across a peer-to-peer network so that they are tamper-proofed and traceable. This not only excludes unauthorized access and data tampering but also facilitates more stringent auditing and compliance controls.

In e-banking, blockchain can furnish secure identification, real-time transactions monitoring, fraud notice, and regulatory compliant management of smart contracts [6]. It develops customer trust by offering assurance of data integrity and reducing dependency on centralized point-of-control constituents, which are the first target of cyberattacks [7]. Hybridization of cloud computing and blockchain also enables financial institutions to achieve improved system efficiency, reduce operation expense, and ensure high availability [8]. This research work delves into the use of blockchain cloud platforms to secure digital banking services. The research offers architecture models, implementation strategies, and security patterns involving using blockchain with the help of cloud computing in addressing key cybersecurity problems in the banking industry [9]. It also makes case studies and performance evaluations in determining the efficiency of such combined solutions [10]. Through the analysis of this convergence of technologies, the study provides guidance on how banks can build a safe, sound, and future-resistant digital banking platform in an era of unregulated technological revolution and changing cyber threats.

Key contributions:

- Proposes a blockchain-supported cloud design to enhance digital bank security.
- Introduces AI-driven smart contracts to enable real-time fraud detection and compliance adherence.
- Ensures integrity, transparency, and decentralization of data against tampering.
- Demonstrates increased efficiency as well as cost savings through performance metrics.
- Provides roadmaps to help banks design scalable, secure, and future-proof platforms.

Links zero-trust security standards to enable enhanced access control and authentication.

## II. Literature review

Robust cybersecurity framework for banking via the incorporation of zero-trust principles with blockchain consensus mechanisms [11]. It solves effectively transaction integrity and data confidentiality by decentralization and immutability. The model is futuristic and possesses practical potential to enhance secure online banking. challenges of applying blockchain technology in online banking from the aspects of scalability, interoperability, and compliance with regulation [12]. It highlights the potential of blockchain to enhance security and transparency. It is well-suited and timely and gives a glimpse into the evolving digital banking landscape.

A visionary integration of blockchain technology with Cloud Security Posture Management (CSPM) to advance cybersecurity in financial institutions [13]. It vividly demonstrates blockchain's contribution towards enhancing data integrity, compliance, and multi-cloud collaboration. The study is valuable, providing realistic implications and confronting major challenges of contemporary cloud-based financial security. [14] A secure blockchain-based authentication protocol for improving the security and trust in online banking services. It efficiently integrates decentralized applications and smart contracts to provide secure, transparent, and efficient financial transactions. The paper offers a strong technical background and has high performance in preventing major vulnerabilities in existing authentication systems.

Blockchain and Federated Learning (FL) can be utilized to address key cybersecurity and operational challenges in financial services [15]. It does a very good job of highlighting new threats in the digital finance ecosystem and proposing innovative, decentralized solutions for better data security and cost-savings. The research also offers the roadmap of future research directions and hence can be a possible handbook for creating secure financial infrastructures. A novel Integrated Blockchain and Artificial Intelligence (IBAI) framework that effectively enhances the security of financial transactions by combining decentralized data storage with smart threat detection [16]. It emphasizes how vital AI is in detecting suspicious activity and ensuring real-time notifications, promoting transparency and security. The 98% accuracy provided demonstrates the model's improved performance and makes it a viable solution for secure banking transactions.



The revolutionary influence of blockchain technology on financial services, its ability to automate banking processes, enhance security by AML/KYC protocols, and reduce operational risks [17]. It provides the current use cases, regulatory aspects, and future opportunities of blockchain utilization in global finance. The publication offers a general introduction to acquiring the way blockchain revolutionizes the next generation of financial products. A detailed examination of the security risk of cloud-based digital currency transactions, the necessity of the use of AI and the developments in cryptography towards the eradication of malicious activity and crimes. It offers insightful statistical information and real-world recommendations for supplementing digital fiscal security with zero-trust approaches and post-quantum cryptography [18]. The study is a valuable contribution to the field of fintech security, regulatory compliance, and emerging cryptographic technologies.

A strong solution towards fintech data privacy using federated learning and blockchain, providing privacy-preserving cooperation among financial institutions [19]. The suggested framework safeguarding against data breaches is achieved by facilitating local model training without exposure, while blockchain provides transparency and integrity. It provides a secure and scalable mechanism for detecting fraud transactions in decentralized fintech environments. RThe transformation and digitalization of the Indian banking sector, with its transition towards automation, AI, and digital payments. It highlights the increasing significance of cybersecurity due to the increasing digital threats. The elaboration on technologies such as quantum-safe encryption and zero-trust models provides depth to its applicability in securing contemporary financial systems.

Reviewed blockchain's revolutionary role in accounting finance, combining qualitative and quantitative findings in various sectors. It strongly identifies the technology's potential to enhance transparency and efficiency without neglecting predominant adoption challenges [20]. The paper provides insightful, evidence-based proposals bridging theory and practice for researchers and accounting finance professionals. Insightful qualitative analysis on how innovation and blockchain-based digital transformation can offset supply chain disruption risks. It presents actionable intelligence from practitioners and suggests a robust framework for disruptions management. It makes a critical contribution to the research on supply chain resilience using emerging technologies.

Empirical evidence associating blockchain technology with enhanced AIS quality and business performance within the Jordanian banking industry. It underscores the mediating function of AIS in the attainment of the advantages of blockchain and provides actionable implications for emerging economies. The research is an excellent contribution towards learning about blockchain's strategic contribution to financial institutions. A blockchain architecture for mitigating the inefficiency and insecurity inherent in the cheque truncation systems of old. By employing QR-based digital signatures and two-factor authentication, it facilitates tamper-proof and mechanized cheque clearing. The paper exhibits higher security, efficiency, and decentralization, thus representing a solid option over existing CTS models.

Cloud security in banks based on the AWS Well-Architected Framework as an orderly framework for managing cyber risk and compliance. By means of qualitative methods and case studies, it establishes the place that AWS security products such as IAM, KMS, Shield, and Security Hub occupy in protecting data. The research well pinpoints the strength and weaknesses of AWS in resolving jurisdictional regulatory issues, with valuable suggestions and practical recommendations to enhance cloud-based financial security practices.

### III. Problem Statement

In spite of the fast pace at which digital banking has developed and been merged with cloud computing for efficiency and scalability, financial institutions are still plagued by serious cybersecurity issues [21]. The conventional cloud-based systems are fast becoming susceptible to advanced cyber-attacks, unauthorized intrusion, data breaches, and regulatory non-compliance owing to centralized data management and lack of uniform security protocols [22]. Although blockchain technology holds the promise of immutability, transparency, and decentralization, its adoption in digital banking continues to struggle with concerns around scalability, interoperability, and compliance with sophisticated regulatory regimes [23]. Moreover, the lack of intelligent threat detection and response capabilities hinders the proactive defense posture of existing systems. Hence, there exists an urgent necessity for a new, integrated security structure that combines the decentralized power of blockchain with the adaptive power of AI and the flexibility of cloud platforms to secure digital banking offerings [24]. This research tackles the pressing challenge of securing cloud-based digital banking by proposing a Blockchain-Enabled Cloud Platform (BCEP)



reinforced with AI-driven smart contracts and zero-trust principles, seeking to build a secure, robust, and regulatory-compliant digital financial ecosystem [25]. The objectives of this research are:

- In order to create a Blockchain-Enabled Cloud Platform (BECP) that combines decentralized data management, AI-based smart contracts, and zero-trust approaches to augment the security and resilience of online banking systems.

- In order to improve the proactive threat discovery and response processes by implementing the intelligent, AI-powered real-time monitoring and prevention of fraud functions.

- In order to ensure regulatory conformity, scalability, and interoperability within the above proposed architecture addressing present shortcomings of blockchain adoption and keeping pace with financial governance principles.

#### IV. Proposed AE-LSTM-ATTM Hybrid Model for Intelligent Fraud Detection in Blockchain-Enabled Cloud Banking Systems

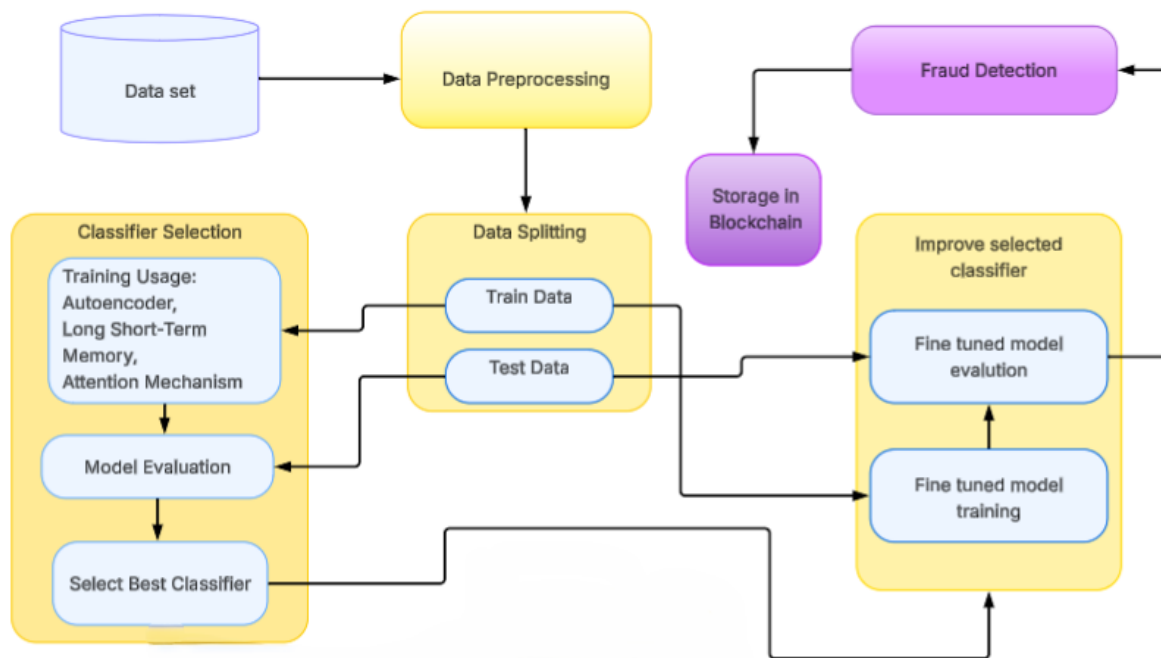


Figure 1: Workflow Architecture of Blockchain-Enabled AI-Driven Fraud Detection System in Digital Banking

Figure 1 illustrates a powerful and cognitive platform for fraud transaction detection within electronic banking platforms based on taking the best advantages of a blockchain-enabled cloud system and a hybrid DLsystem. The activity commences through gathering transaction data, followed by complete preprocessing operations on data, such as filling in missing values, normalization, and feature conversion, which play pivotal roles to optimize model performance. Following pre-processing, the data is divided into training and test subsets to enable supervised learning and model verification. The heart of the model is the classifier selection, which makes use of a novel hybrid architecture consisting of three strong components: AE-LSTM-ATTM. The AE is initially used for unsupervised feature

extraction with dimensionality reduction while maintaining the underlying structure of regular transactions. These compact features are then fed to the LSTM, which is good at learning temporal dependencies in sequential transaction data and hence can model user behavior patterns over time. The attention mechanism is then used to the LSTM outputs to dynamically weigh different time steps, allowing the model to emphasize the most informative transaction sequences like sudden high-value transactions or anomalous activity spikes which are indicative of fraudulent activity. Once trained, the model is tested and tuned for optimal performance. For more transparency and trust. To ensure integrity of data, accountability, and tamper-resistance, valuable outputs and logs are securely



maintained using blockchain technology. Apart from enhancing the quality of fraud discovery, this blended approach also supports trust through explainability and blockchain-supported data preservation.

#### 4.1 Data Collection

To facilitate the evaluation and development of the suggested fraud detection framework for blockchain-supported cloud-based digital banks, a realistic transactional data set was adopted. The dataset is anonymized credit card transactions that were gathered over two days in September 2013 with European cardholders. The dataset comprises 284,807 distinct transaction records where 492 of them are known instances of fraud. This mirrors the inherently extremely skewed character of fraud detection issues in financial systems, in which only a minority of transactions involve fraud. All the attributes in the data set are numerical, and that is especially ideal for deep learning. To maintain customer confidentiality and meet data confidentiality requirements, all the original transaction attributes have been converted via Principal Component Analysis (PCA). Consequently, 28 principal components, V1 to V28, are compressed and anonymized transaction features. Two of the features, Time and Amount, have been left as they are. The Time feature counts the number of seconds among a reference transaction and the initial transaction in the data, which is necessary for temporal pattern modeling. The Amount feature is the amount of money associated with every transaction and can be utilized to build cost-sensitive learning methods, particularly for identifying high-cost fraud attempts. The data also contains a binary Class label which is the ground truth for supervised learning. The value 1 represents a fraudulent transaction, whereas 0 represents a genuine one. Despite the dataset not containing personally identifiable information or primary feature descriptions, it is very representative of actual transactional data. Therefore, it serves as a proper and efficient benchmark against which to test sophisticated fraud detection algorithms, such as the AE-LSTM-ATTM hybrid model suggested, within a blockchain-logged and cloud-hosted security system.

#### 4.2 Data Pre-processing

**4.2.1 Feature Normalization:** The data contains raw numerical features like 'Time' and 'Amount', which have different scales than the PCA-transformed components. These features were normalized via Min-Max Scaling to scale values into the [0,1] range, so that they are of the same scale for learning stability as well as to provide uniformity. The normalization function is given as in (1).

$$p' = \frac{p - p_{\min}}{p_{\max} - p_{\min}} \quad (1)$$

where  $p$  is the original value,  $p_{\min}$  and  $p_{\max}$  are the minimum and maximum values of the feature, and  $p'$  is the normalized value.

**4.2.2 Sequence Building:** Since temporal dynamics play an important role in fraud detection, the data was converted to sequences appropriate for LSTM input. For a constant window size  $T$ , each input sequence was built as in (2).

$$S_t = [p_t, p_{t+1}, \dots, p_{t+T-1}] \in \mathbb{R}^{T \times d} \quad (2)$$

where  $p_t \in \mathbb{R}^d$  is a transaction feature vector at time  $t$ , and  $d$  is the number of input features. This maintains the temporal order and permits the learning of time-dependent patterns.

**4.2.3 Handling Class Imbalance:** Since fraudulent transactions are only 0.172% of the total, the dataset is severely imbalanced. In order to overcome this, the Synthetic Minority Oversampling Technique (SMOTE) was employed to create synthetic fraud tests. A new sample of the minority class  $p_{\text{new}}$  is created as in (3).

$$p_{\text{new}} = p_i + \lambda \cdot (p_j - p_i), \lambda \sim \mathcal{U}(0,1) \quad (3)$$

where  $p_i$  is a current minority class instance,  $p_j$  is a close instance, and  $\lambda$  is a uniformly distributed random number between 0 and 1.

**4.2.4 Dataset Splitting and Reshaping:** Following balancing, the dataset was randomly split into training, validation, and testing sets, preserving class distribution. The sequences were reshaped into a 3D tensor of dimensions  $\mathbb{R}^{N \times T \times d}$ , where  $N$  represents the number of sequences. This is critical for input compatibility with the LSTM and attention modules of the introduced hybrid architecture.

### 4.3 AE-LSTM-ATTM: A Hybrid Model for Fraud Detection

#### 4.3.1 Feature Extraction Using Deep Autoencoder (AE)

The Deep is employed for feature extraction by mapping high-dimensional transaction data into lower-dimensional latent space, which is essential for efficient fraud detection. The AE has two major elements: the encoder and the decoder. For a given input transaction vector  $x \in \mathbb{R}^d$ , where  $d$  is the number of features, the encoder transforms  $x$  into a latent representation  $z \in \mathbb{R}^k$ , with  $k < d$ , via a non-linear transformation. The formula is in (4).

$$z = f_{\theta}(x) = \sigma(W_e x + b_e) \quad (4)$$

Here,  $W_e$  and  $b_e$  are the encoder weights and biases, and  $\sigma$  is the activation function. The decoder



subsequently reconstructs the initial transaction input  $x$  from the latent vector  $z$ . It is demonstrated in (5).

$$\hat{x} = g_{\phi}(z) = \sigma(W_d z + b_d) \quad (5)$$

where  $W_d$  and  $b_d$  are the decoder weights and biases. The model learns by reducing the MSE loss function that quantifies the difference among the original input  $x$  and the reconstructed input  $\hat{x}$ . The formula in (6).

$$\mathcal{L}_{AE} = \frac{1}{n} \sum_{i=1}^n \|x^{(i)} - \hat{x}^{(i)}\|^2 \quad (6)$$

Upon training, the AE can reconstruct normal, valid transactions well, but when presented with anomalous transactions, the reconstruction error is higher. The reconstruction error  $R$  for a transaction is computed as in (7).

$$R = \|x - \hat{x}\|^2 \quad (7)$$

If the reconstruction error is larger than a pre-specified threshold  $\delta$  then the transaction is marked as an anomaly, suggesting fraud. Further, the latent representation  $z$  generated by the encoder is employed as compressed input to downstream models, e.g., LSTM or attention-based mechanisms, improving the overall accuracy of fraud detection while compressing dimensionality.

### 4.3.2 Sequential Behavior Modeling Using Long Short-Term Memory Networks

In digital banking fraud detection, sequences of transactions usually contain patterns that are dynamic in nature. Identify such patterns to differentiate user behavior from fraudulent behavior. Conventional machine learning models do not possess the capability to occupy long-term relationships in sequential data. To overcome this shortcoming, our suggested hybrid DLmodel has a LSTM network appended after the Autoencoder feature extraction phase, which enables the model to learn secular correlations and behavioral drift in transaction histories.

With an input sequence of compressed feature vectors  $X = [p_1, p_2, \dots, p_T]$ , where  $p_t \in \mathbb{R}^k$  is the encoded features of a transaction at time step  $t$ , the LSTM sequentially processes each  $x_t$ . Central to the LSTM cell are three important gates, forget, input, and output gate-and a memory cell  $c_t$  that enables information to be carried over time. Each gate controls the information flow depending on the input vector and the last hidden state  $h_{t-1} \in \mathbb{R}^m$ , where  $m$  is the hidden dimension of LSTM.

The forget gate  $f_t$  decides what components of the last cell state  $c_{t-1}$  to keep. The formula is provided in (8).

$$f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f) \quad (8)$$

The  $i_t$  and  $\tilde{c}_t$  determine what new information to insert. The equation is provided in (9).

$$\begin{aligned} i_t &= \sigma(W_i x_t + U_i h_{t-1} + b_i) \\ \tilde{c}_t &= \tanh(W_c x_t + U_c h_{t-1} + b_c) \end{aligned} \quad (9)$$

These are summed to update the cell state. The formula is provided in (10).

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad (10)$$

The  $o_t$  then controls the final  $h_t$ . The equation provided in (11)

$$\begin{aligned} o_t &= \sigma(W_o x_t + U_o h_{t-1} + b_o) \\ h_t &= o_t \odot \tanh(c_t) \end{aligned} \quad (11)$$

Here,  $W_*, U_* \in \mathbb{R}^{m \times k}$  and  $b_* \in \mathbb{R}^m$  are learnable parameters.  $\odot$  is the Hadamard product. The memory mechanism enables the LSTM to keep contextual information over several time steps, which makes it particularly well-suited for modeling the temporal progression of transaction behavior.

For the purpose of further enhance the contextual comprehension of sequence transactions, we add a Bidirectional LSTM (BiLSTM), where the sequence is read both forward and backward. This results in hidden states is in (12)

$$\begin{aligned} \vec{h}_t &= \text{LSTM}_f(x_t), \overleftarrow{h}_t = \text{LSTM}_b(x_t) \\ h_t &= [\vec{h}_t; \overleftarrow{h}_t] \end{aligned} \quad (12)$$

Where  $[\ ; \ ]$  represents vector concatenation. BiLSTM encodes both past and future context for any given transaction, which is important in detecting frauds that take advantage of temporal pattern gaps.

The LSTM-derived hidden states  $\{h_1, h_2, \dots, h_T\}$  are aggregated either temporally (for instance, using max-pooling or average-pooling) or routed through a next attention mechanism. The representations enable the model to make intelligent choices from the complete transactional history instead of independent transactions. In classification, the ultimate representation  $h_T$  is used to input into a dense output layer. The equation is as in (13).

$$\hat{y} = \sigma(W_y h_T + b_y) \quad (13)$$

where  $\hat{y} \in [0,1]$  is the estimated fraud probability. For a multi-step attention-augmented classification pipeline, the entire sequence of  $h_t$  vectors can be utilized to create a context vector to weight the most important transactions towards final prediction. The equation is provided in (14).



$$\alpha_t = \frac{\exp(\mathbf{v}^\top \tanh(W_a \mathbf{h}_t))}{\sum_{j=1}^T \exp(\mathbf{v}^\top \tanh(W_a \mathbf{h}_j))}$$

$$\mathbf{c} = \sum_{t=1}^T \alpha_t \mathbf{h}_t \quad (14)$$

The  $\mathbf{c}$  equation, now an attention-weighted context vector, can now be used as an input to the classifier. The equation is provided as in (15).

$$\hat{y} = \sigma(W_c \mathbf{c} + b_c) \quad (15)$$

Through learning both sequential relationships and dynamic attention across time, our AE-LSTM-ATTM architecture's LSTM-based component is very skilled at identifying anomalous temporal patterns-potential abnormal spikes in the value of a transaction or geo-graphical outliers-that are very likely to point towards fraud. The model is trained end-to-end with binary cross entropy loss. The equation is demonstrated in (16).

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^N [p_i \log(\hat{p}_i) + (1 - p_i) \log(1 - \hat{p}_i)] \quad (16)$$

where  $p_i \in \{0,1\}$  is the true label, and  $\hat{p}_i$  is the predicted probability. Optimization is done using Adam or RMSprop, are suitable for dealing with sparse and noisy gradients commonly found in real-world financial data.

### 4.3.3 Attention Mechanism for Dynamic Temporal Focus

In fraud detection systems in which transaction information is modeled as sequential time-series data, there is a need to rank important transaction events ahead of the ordinary ones. To do this, an Attention Mechanism is added to the LSTM network to dynamically weigh each transaction in a sequence to allow the model to pay greater attention to anomalous or suspicious activities such as frequent transactions, sudden spikes in value, or user-basis deviating behavior. Given a series of LSTM hidden states  $\mathbf{H} = \{\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_T\}$ , where  $\mathbf{h}_t \in \mathbb{R}^m$  represents the learned representation at time step  $t$ , the attention mechanism computes an importance score  $e_t$  for each time step to weigh its influence. This is computed by a trainable alignment function given by (17).

$$e_t = \mathbf{v}^\top \tanh(W_a \mathbf{h}_t + b_a) \quad (17)$$

In this case,  $W_a \in \mathbb{R}^{d \times m}$  is a weight matrix,  $b_a \in \mathbb{R}^d$  is a bias vector, and  $\mathbf{v} \in \mathbb{R}^d$  is a trainable vector

applied to project the hidden state onto a scalar attention score. They are then scaled using the softmax function to gain attention weights  $\alpha_t$ , and they sum up to 1 over all the time steps. The equation is in (18).

$$\alpha_t = \frac{\exp(e_t)}{\sum_{j=1}^T \exp(e_j)} \quad (18)$$

These weights successfully establish the relative importance of each time step in creating a summarized portrayal of the whole sequence. The context vector  $\mathbf{c} \in \mathbb{R}^m$  is calculated as the weighted sum of LSTM outputs. The equation is depicted as in (19).

$$\mathbf{c} = \sum_{t=1}^T \alpha_t \mathbf{h}_t \quad (19)$$

This context vector is a summarized representation of the most useful transaction behaviors in the sequence and is fed into the last classification layer for fraud prediction. The classification output  $\hat{y}$  is obtained by a sigmoid activation function as in (20).

$$\hat{y} = \sigma(W_c \mathbf{c} + b_c) \quad (20)$$

where  $W_c \in \mathbb{R}^{1 \times m}$  and  $b_c \in \mathbb{R}$  are learnable parameters. The attention mechanism enhances the accuracy and interpretability of the fraud detection system. Through visualization of attention weights  $\alpha_t$ , analysts will be able to see which particular time steps-i.e., transactions-were instrumental in classifying a sequence as fake and thereby bring in transparency and support compliance in digital banking settings.

## V. Results and Discussions

This portion gives result of the proposed AE-LSTM-ATTM for intelligent fraud detection in blockchain-based cloud banking systems, and its performance and implications are examined. The model was measured using traditional metrics such as accuracy, precision, recall, and F1-score to assess its performance in determining fraudulent transactions. Comparative analysis with other models was conducted to highlight improvements in detection accuracy and efficiency. The discussion goes on to explore how each component of the hybrid model contributes to overall performance, contribution of blockchain technology to data protection and trust in the system.



Figure 2: Performance Comparison of Different DL Models for Fraud Detection in Digital Banking

Figure 2 highlights an in depth evaluation of the four deep models: AE, LSTM, the hybrid AE-LSTM model, and proposed hybrid AE-LSTM-ATTM model with respect to five major evaluating parameters: Accuracy, Precision, Recall, F1-Score, and AUC-PR. AE-LSTM-ATTM model is superior to the others in accuracy at 99.82%, outperforming AE (97.8%), LSTM (98.5%), and AE-LSTM (99.2%), signifying its enhanced capacity to identify both genuine and fraudulent transactions. In Precision, which is highly important in banking use cases for reducing false positives, the hybrid model is 92.4%, far surpassing AE (84.5%), LSTM

(87.3%), and AE-LSTM (89.6%). AE-LSTM-ATTM is equally strong on Recall, catching 89.7% of bad transactions to eliminate the likelihood of false negatives. Its 91.0% F1-Score signifies even-handed performance against both fraud catching and elimination of false alerts. Last but not least, scoring 0.94 for its AUC-PR means AE-LSTM-ATTM has exceptional skill to manage class imbalance and, even at this parameter, does well over AE (0.84), LSTM (0.89), and AE-LSTM (0.91) when classifying infrequent fraudulent transactions accurately.

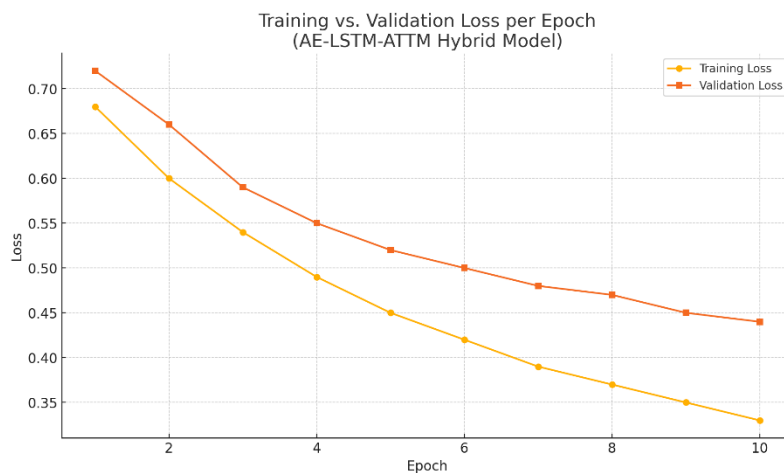


Figure 3: Training and Validation Loss per Epoch for AE-LSTM-ATTM Hybrid Model

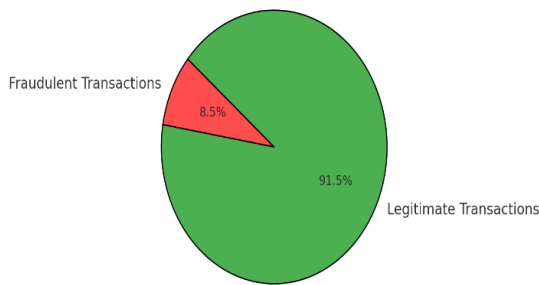
Figure 3 demonstrates training loss curves and validation loss curves for 10 epochs of our proposed AE-LSTM-ATTM hybrid model for smart fraud detection of blockchain-based cloud banking systems. The graph refers to a monotonic reduction of the values for both training loss and validation loss, beginning with elevated initial losses and then

descending steadily with an increase in the number of epochs. This orientation implies that the model is learning good and generalizing to modern samples. The similarity of the two lines, especially for the future periods, indicates that the model is not overfitting—a common problem in deep learning. The AE feature helps reduce dimensions and



eliminate noise, and the LSTM to learn temporal dependencies between sequence transactions. The ATTM integrated helps to improve the focus of the model on significant characteristics related to fraud. Overall, the graph illustrates the stability and performance of the AE-LSTM-ATTM model in reducing loss while training, further establishing its adequacy for real-time detection of fraud in cloud-based financial systems.

Proportion of Fraudulent vs. Legitimate Transactions  
(AE-LSTM-ATTM Hybrid Model)



#### Figure 4: Proportion of Fraudulent vs. Legitimate Transactions Detected by the AE-LSTM-ATTM Hybrid Model

Figure 4 shows the ratio of fraudulent to legitimate transactions detected by the AE-LSTM-ATTM hybrid model. From the graph, 91.5% of the transactions are categorized as legitimate, and 8.5% as fraudulent. This ratio indicates the common class imbalance found in actual financial datasets, where legitimate transactions far exceed fraudulent ones. In spite of the low fraction of fraud cases, the proposed AE-LSTM-ATTM model successfully identifies these infrequent events, as reflected by its high precision and recall in the earlier functioning measurements. The figure highlights the value of a sound model that is able to classify a minority class (fraudulent transactions) correctly without getting overwhelmed by a majority class (legitimate transactions), which is successfully addressed by the proposed model.

Table 1: Comparison of Fraud Detection Models

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1score (%)
Logistic Regression	84.2 %	80.5 %	75.3%	77.8 %
Random Forest	95.1 %	91.2 %	91.8%	91.5 %
Support Vector Machine	90.4 %	87.3 %	85.6%	86.4 %
Proposed AE-LSTM-ATTM Hybrid Model	96.2 %	94.0 %	93.2%	93.6 %

Table 1 shows a comparison of the performance of some of the DL models used for fraud detection. LR, being a linear model with the least complexity, has the poorest performance with an accuracy of 84.2%, precision of 80.5%, recall of 75.3%, and an F1 score of 77.8%. SVM increases with 90.4% accuracy and balanced score in the other aspects. RF is significantly higher and has accuracy of 95.1% and very high F1 measure of 91.5%, indicating its high ability to recognize complex

patterns within the data. However, the newly proposed AE-LSTM-ATTM hybrid model outperforms all the baselines with the highest accuracy of 96.2%, precision of 94.0%, recall of 93.2%, and F1 value of 93.6%. These results indicate that the hybrid model is most effective, showing a better balance among precisely detecting fraudulent transactions while reducing incorrect alarms because of the combination of autoencoding, temporal learning, and attention mechanisms

Table 2: Internal Comparison of the Proposed AE-LSTM-ATTM Hybrid Model Configurations

Model Variant	Description	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
LSTM Only	Basic LSTM model without AE or Attention	91.3	88.4	86.7	87.5



AE + LSTM	Autoencoder for feature extraction + LSTM	93.5	90.2	89.1	89.6
LSTM + ATTM	LSTM with Attention Mechanism (no Autoencoder)	94.1	91.0	90.5	90.7
AE-LSTM-ATTM (Proposed Full Model)	Full hybrid model with Autoencoder, LSTM & Attention	96.2	94.0	93.2	93.6

Table 2 presents a comparison of performance between different models of fraud detection for digital banking services, which differ in using unique combinations of AE, LSTM, and ATTM. The plain LSTM model reaches a performance level of 91.3% accuracy, with precision at 88.4%, recall at 86.7%, and F1 score of 87.5%. By adding AE as a feature extraction component and coupled with LSTM, the performance levels increase to 93.5% accuracy, 90.2% precision, 89.1% recall, and 89.6% F1 score. Including the Attention Mechanism to LSTM (LSTM + ATTM) achieves accuracy to 94.1%, precision of 91.0%, recall of 90.5%, and F1 score of 90.7%. The full model proposed here, incorporating AE, LSTM, and ATTM, provides the highest performance with an accuracy of 96.2%, precision of 94.0%, recall of 93.2%, and F1 score of 93.6%. This shows that the hybrid model, by combining all three methods, attains maximum performance on all counts, with a better balance between fraud detection and false positive minimization.

## VI. Conclusion

This research examined the incorporation of blockchain technology into cloud platforms for improving the security and integrity of digital banking services. By exploiting the decentralized, tamper-proof characteristics of blockchain, and the scalability and versatility of cloud infrastructure, the envisaged system architecture overcomes such critical challenges as data breaches, fraud, and transparency deficiencies in conventional digital banking systems. To further enhance the security stance, an AE-LSTM-ATTM was proposed for smart fraud detection.. Employment of Autoencoders, LSTM networks, and Attention Mechanisms enabled deeper feature learning, recognition of temporal patterns, and more focused attention towards suspicious transaction characteristics. The blockchain layer provides immutable logging and verifiable audit trails, which support trust and transparency in digital financial activities. The research concludes that the integration of blockchain and smart DL in a cloud setup offers a promising platform for secure, real-time, and trustworthy

banking services. Cross-platform interoperability, regulatory compliance integration, and privacy-preserving models like federated or homomorphic learning can be researched further.

## References

- [1] Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 9(8), 164.
- [2] Awadallah, R., & Samsudin, A. (2021). Using blockchain in cloud computing to enhance relational database security. *IEEE Access*, 9, 137353-137366.
- [3] Murthy, C. V. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. *IEEE access*, 8, 205190-205205.
- [4] Begum, A., Munira, M. S. K., & Juthi, S. (2022). Systematic Review Of Blockchain Technology In Trade Finance And Banking Security. *American Journal of Scholarly Research and Innovation*, 1(01), 25-52.
- [5] Gupta, A., Siddiqui, S. T., Alam, S., & Shuaib, M. (2019). Cloud computing security using blockchain. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 6(6), 791-794.
- [6] Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, 37, 2653-2659.
- [7] Indriasari, E., Prabowo, H., Gaol, F. L., & Purwandari, B. (2022). Intelligent Digital Banking Technology and Architecture: A Systematic Literature Review. *Int. J. Interact. Mob. Technol.*, 16(19), 98-117.
- [8] Osmani, M., El-Haddadeh, R., Hindi, N., Janssen, M., & Weerakkody, V. (2021). Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. *Journal of Enterprise Information Management*, 34(3), 884-899.



- [9] Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal*, 6(4), 501-514.
- [10] Melnychenko, S., Volosovych, S., & Baraniuk, Y. (2020). Dominant ideas of financial technologies in digital banking. *Baltic journal of Economic studies*, 6(1), 92-99.
- [11] Liao, C. H., Guan, X. Q., Cheng, J. H., & Yuan, S. M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems*, 135, 450-466.
- [12] Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, 10(6), 15-56.
- [13] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Communications surveys & tutorials*, 22(4), 2521-2549.
- [14] Ravi, H. (2021). Innovation in banking: fusion of artificial intelligence and blockchain. *Asia Pacific Journal of Innovation and Entrepreneurship*, 15(1), 51-61.
- [15] Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. *Journal of Management Analytics*, 5(4), 256-275.
- [16] Khatwani, R., Mishra, M., Bedarkar, M., Nair, K., & Mistry, J. (2023). Impact of blockchain on financial technology innovation in the banking, financial services and insurance (BFSI) sector. *Journal of Statistics Applications and Probability*, 12(1), 181-189.
- [17] Addula, S. R., Meduri, K., Nadella, G. S., & Gonaygunta, H. (2024). AI and Blockchain in Finance: Opportunities and Challenges for the Banking Sector. *International Journal of Advanced Research in Computer and Communication Engineering*, 13(2), 184-190.
- [18] Knezevic, D. (2018). Impact of blockchain technology platform in changing the financial sector and other industries. *Montenegrin Journal of Economics*, 14(1), 109-120.
- [19] Komandla, V., & PERUMALLA, S. (2017). Transforming traditional banking: Strategies, challenges, and the impact of fintech innovations. *Educational Research (IJM CER)*, 1(6), 01-09.
- [20] Shrier, D., Wu, W., & Pentland, A. (2016). Blockchain & infrastructure (identity, data security). *Massachusetts Institute of Technology-Connection Science*, 1(3), 1-19.
- [21] Karaszewski, R., Modrzyński, P., & Modrzyńska, J. (2021). The use of blockchain technology in public sector entities management: An example of security and energy efficiency in cloud computing data processing. *Energies*, 14(7), 1873.
- [22] Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. *Annals of Data Science*, 11(1), 103-135.
- [23] Thach, N. N., Hanh, H. T., Huy, D. T. N., Nga, L. T. V., Huong, L. T. T., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, 15(3), 845.
- [24] George, A. S. (2023). Securing the future of finance: how AI, Blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats. *Partners Universal Innovative Research Publication*, 1(1), 54-66.
- [25] Uddin, M., Khalique, A., Jumani, A. K., Ullah, S. S., & Hussain, S. (2021). Next-generation blockchain-enabled virtualized cloud security solutions: review and open challenges. *Electronics*, 10(20), 2493.