Kuwait Journal of Advanced Computer Technology
ISSN: 2984-7907
Vol 4 Issue 1 (2026)

Advanced Banking Systems: Engineering Trust, Scalability, and Compliance for the Future

Archana Todupunuri

Fidelity Information Services, USA.

Submitted: 01/02/2026 **Revised:** 15/02/2026 **Published:** 25/02/2026

Abstract:

This paper discusses the engineering remedies that are needed in the creation of the next-generation banking systems that focus on trust, scale, and compliance. It explores the use of machine learning, cloud computing, and blockchain capabilities to improve the processing of transactions and detection of fraud. The study involves predicting the behavior of the customers using LSTM, as well as the normalization techniques enhance the accuracy of models. The study helps to create better, high-performance, scalable, and secure banking platforms in the future by addressing the issue of scalability and security.

Keywords: Advanced Banking Systems, Trust, Scalability, Regulatory Compliance, Machine Learning, LSTM, Fraud Detection, Blockchain, Cloud Computing, Data Normalization, Transaction Processing, Performance Metrics, Financial Technology, AI, Compliance Monitoring.

1. Introduction

The development of banking systems is necessary to address the increasing needs of the digital transformation, with the necessity to provide trust, scale, and regulatory compliance. As the banking environment evolves, conventional banking institutions need to respond through the development of sophisticated systems that offer high-performance solutions and ensure that they remain on the right track to meet the regulatory requirements. Reliability is essential, and it is imperative that banking systems work smoothly and without fail, even when the traffic is high as well as during complicated transactions [1]. Scalability is also significant to ensure efficient growth that is capable of supporting the rising customer needs and transactions [2]. Moreover, now regulatory compliance has become one of the priority points, particularly due to the emergence of strict data privacy legislation and other financial legislation.

1.1 Problem Statement

The fast change of the banking industry requires the creation of new sophisticated systems that guarantee confidence, scalability and compliance to the regulations. The existing systems usually cannot make these vital needs come into equilibrium with each other, resulting in a lack of efficiency and possible security threats [3]. This study seeks to deal with the issues of establishing banking systems that are not only safe but also have the capacity to support more load and sustainable systems that are consistent with the rigorous regulation systems to guarantee sustainability in the long term.

1.2 Research Contribution

The study will add to the knowledge on the development of the next generation of banking engineering solutions. It is interested in the creation of frameworks and methods to increase the reliability, scalability, and compliance of banking platforms. The results will inform about the good practices of developing secure, efficient systems, establishing compliance with regulatory standards to benefit not only the financial institutions but also their customers and establishing trust and efficient operation.

1.3 Objectives

- To explore the most important engineering concepts that can lead to the creation of stable and high-performance banking systems.
- To examine regulatory compliance that affects the design and operation of the banking platforms.
- To evaluate the performance and scalability requirements of next-generation banking systems.
- To come up with a novel idea of solving the dilemma of trust, scale, and compliance in the banking systems.

2. Literature Review

2.1 Next-Generation Banking Systems' Trust and Security

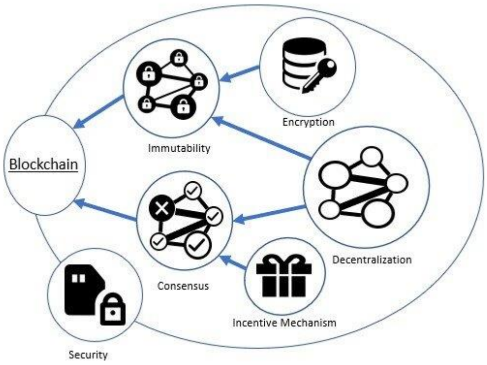


Figure 1: Blockchain Security Architecture of the Banking System

Trust and security are the pillars of the modern banking systems. The privacy, integrity and accessibility of data are the most important aspects in the growing digitalization of financial transactions [4]. The systems should have strong encryption and authentication and access control protocols to ensure that sensitive customer details and money are not lost. Studies have indicated that the banking industry is vulnerable to data breaches, cyber-attacks, and fraud as some of the critical risks. More recent technologies, such as blockchain and artificial intelligence (AI), are being implemented to solve these security concerns, as they provide decentralized and incredibly secure solutions to them [5]. The principle of zero-trust security models is under development, where the principle presupposes a security that revolves around the idea that all the requests that the network receives can be considered a threat [6].

2.2 Banking Systems Scalability and Performance

The banking systems need to be scaled to boost their efficiency as the financial industry undergoes a high growth rate. Scalability guarantees that the systems are able to offer services to increased numbers of customers, very high volumes of transactions as well as very complex processes of data processing [7]. The use of cloud computing, microservices architecture, and containerization is becoming more and more popular to generate flexible and scalable banking systems [8].

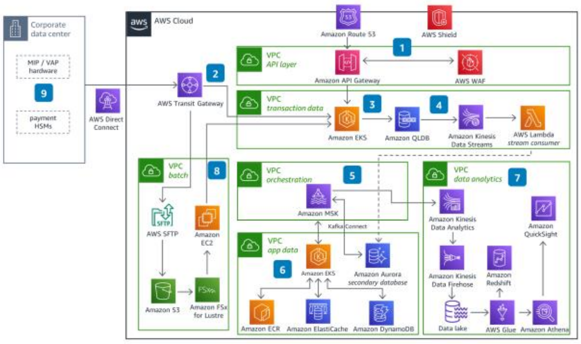
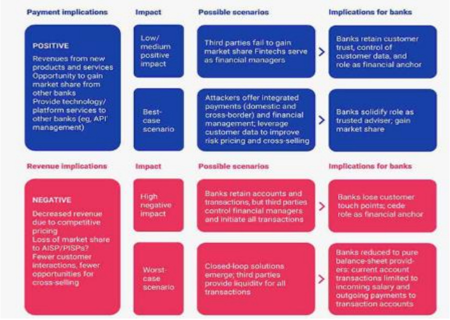


Figure 2: Core Banking System using AWS

The image contains an example of a strong AWS cloud setup, which combines such elements as API Gateway, Kinesis Data Streams, Lambda, and DynamoDB to process real-time data, perform secure transactions and scale-out infrastructure. It facilitates complex banking systems with improved performance, security, and compliance with the solutions on cloud.

2.3 Risk Management and Regulatory Compliance



Payment implications	Impact	Possible scenarios		Implications for banks
POSITIVE Revenues from new products and services Opportunity to gain market share from other banks Provide technology/ platform services to other banks (eg, API' management)	Low/ medium positive impact	Third parties fail to gain market share Fintechs serve as financial managers	>	Banks retain customer trust, control of customer data, and role as financial anchor
	Best-case scenario	Attackers offer integrated payments (domestic and cross-border) and financial management; leverage customer data to improve risk pricing and cross-selling	>	Banks solidify role as trusted adviser; gain market share

Revenue implications	Impact	Possible scenarios		Implications for banks
NEGATIVE Decreased revenue due to competitive pricing Loss of market share to AISP/PISPs? Fewer customer interactions, fewer opportunities for cross-selling	High negative impact	Banks retain accounts and transactions, but third parties control financial managers and initiate all transactions	>	Banks lose customer touch points; cede role as financial anchor
	Worst-case scenario	Closed-loop solutions emerge; third parties provide liquidity for all transactions	>	Banks reduced to pure balance-sheet provid-ers: current account transactions limited to incoming salary and outgoing payments to transaction accounts

Figure 3: Risk Management using PSD2

Banking is a highly regulated environment, and there are strict policies on the privacy of data, anti-money laundering (AML), as well as the know-your-customer (KYC) policy. Due to changes in regulations, the banking systems should be developed not only as per the present-day compliance requirements but also be flexible to accommodate future changes [9]. In this field, technological factors are also peripherally influencing regulatory technology (RegTech) that is replacing compliance tasks and helping to track transactions in real time in order to detect suspicious activity. The immutability of blockchain also facilitates compliance since it will have transparent audible transaction records [10]. Another important compliance parameter is effective risk management because banks should always look over risks associated with credit, operational and market parameters. An effective banking system has to be crafted with the compliance aspects under consideration, as well as be continually compliant with international standards like GDPR, PSD2, and Basel III [11].

2.4 New Technologies Defining the Future of Banking

The future of next-generation banking systems depends on mingling the emerging technologies. Machine learning (ML) and artificial intelligence (AI) are actively applied to automatize the processes, prevent fraud, and enhance interaction with customers by using chatbot and virtual assistants [12]. The use of AI-based credit scoring models and predictive analytics by banks to make better decisions when lending, minimize risks, and enhance profitability [13]. Also, the emergence of blockchain technology is changing the way transactions are performed, and it is providing decentralized solutions to the processes, minimizing the use of intermediaries and increasing the level of transparency in transactions. Innovation is also promoted with the help of open banking, which is led by the use of API integration and enables third-party providers to develop additional financial products and services [14].

Research Gap

Although progress has been immense in banking systems, there is an evident gap in the literature that would successfully incorporate the aspects of trust, scalability and regulatory compliance into one unit. The current studies tend to discuss these points independently, and little is being done on the joint influence of these points on the design of the system.

3. Methodology

The methodology builds scalable, trustworthy, and compliant machine learning-based banking systems. The important components are the data collection, the pre-processing of the data, the predictive analysis through Long Short-Term Memory (LSTM) networks and the optimization of hyperparameters through Bayesian Optimization [15].

The data gathering will be in the following steps:

Transaction Data: Data on the past transaction history in terms of deposits and withdrawals, transfers, and loan payments will be gathered to understand customer behavior and the future projections of financial success.

Customer Demographics: Demographics about the customers, including their age, income, location and account type, will be collected in order to segment the customer base and make predictions unique to each segment.

Loan Performance: Information regarding the loan approval, repayment schedules, and defaults will be included to forecast the loan performance and credit worthiness by the customers.

Regulatory Compliance Data: To keep the privacy and security standards, the method of collecting data must be regulated by such laws as GDPR and PCI-DSS.

Data Pre-Processing and Normalization

Min-Max normalization is applied to ensure that all features are on the same scale. This prevents any one feature from dominating the model due to large value ranges [16]. The Min-Max normalization formula is:

$$x_{normalised} = \frac{x - x_{min}}{x_{max} - x_{min}}$$

This scaling makes all features equally contribute to the model, which enhances the performance of machine learning models and convergence, especially those that process sequential data such as LSTMs.

Long Short-Term Memory Architecture for Predictive Analysis

LSTM networks are a form of Recurrent Neural Network (RNN) that processes a series of data, like customer transaction history. LSTMs are useful in learning long-term dependencies and virtually eliminating the problem of vanishing gradients during RNNs [17]. The LSTM cell has four main parts, which are input, forget and output gates, with the help of which the information flow is controlled. The mathematical model of the forget gate is:

$$f_t = \sigma(w_f \cdot [h_{t-1}, x_t] + b_f)$$

In which ft represents the output of the forget gate, Wf represents the weight matrix, and σ is the sigmoid function. The architecture is most suitable in banking systems, such as the detection of fraud, predicting loans and also predicting customer behavior.

Hyperparameter Tuning Using Bayesian Optimization

The hyperparameters of the LSTM model optimization are done using Bayesian Optimization (BO). Opinion BO probabilistic models can explore the hyperparameter space efficiently unlike grid or random search which are computationally inefficient [18]. The acquisition function is used to guide the optimization process:

$$\widehat{f}\,(x) = arg\,max\;\; Acquisition(x)$$

This method guarantees the LSTM model stops quicker and operates more effectively through the choice of optimal hyperparameters in an organized manner and enhances the precision and effectiveness of prediction.

LSTM Implementation for Banking Applications

The LSTM model has been applied to different situations in the banking industry, including loan defaults, customer churn, and detecting fraud. LSTM networks are able to make real-time predictions based on historical transaction data, and this helps in decision-making processes while ensuring there is high scalability and compliance [19]. The model is developed using previous data and implemented to make predictions later, which would make the banks stay ahead of customer behavior and market trends.

Scalability and Compliance

The system is scalable and can handle large amounts of transaction data and support expansion in banking operations. It also concerns the adjustment to such regulations as GDPR or PCI-DSS because model predictions are processed in a way that is secure, interpretable, and auditable [20].

Workflow Diagram

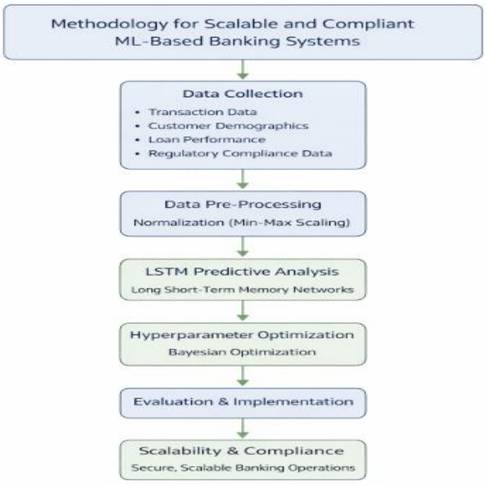
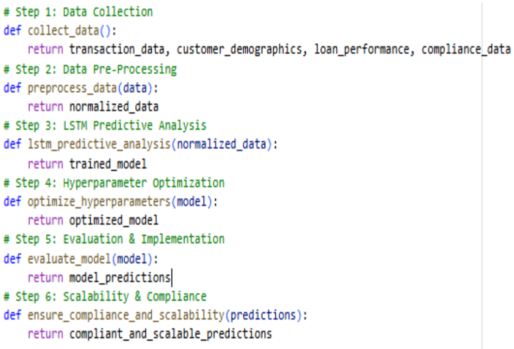

Methodology for Scalable and Compliant ML-Based Banking Systems
Data Collection
• Transaction Data
• Customer Demographics
• Loan Performance
• Regulatory Compliance Data
Data Pre-Processing
Normalization (Min-Max Scaling)
LSTM Predictive Analysis
Long Short-Term Memory Networks
Hyperparameter Optimization
Bayesian Optimization
Evaluation & Implementation
Scalability & Compliance
Secure, Scalable Banking Operations

Figure 4: Workflow Diagram

Pseudocode



```
# Step 1: Data Collection
def collect_data():
    return transaction_data, customer_demographics, loan_performance, compliance_data
# Step 2: Data Pre-Processing
def preprocess_data(data):
    return normalized_data
# Step 3: LSTM Predictive Analysis
def lstm_predictive_analysis(normalized_data):
    return trained_model
# Step 4: Hyperparameter Optimization
def optimize_hyperparameters(model):
    return optimized_model
# Step 5: Evaluation & Implementation
def evaluate_model(model):
    return model_predictions
# Step 6: Scalability & Compliance
def ensure_compliance_and_scalability(predictions):
    return compliant_and_scalable_predictions
```

Figure 5: Pseudocode

4. System Architecture:

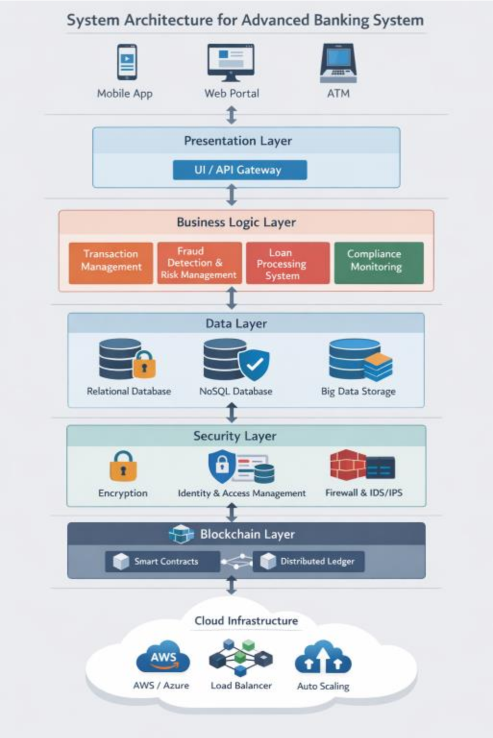


Figure 6: System Architecture

4.1 Client Layer:

The end users make their interaction with the banking system at the Client Layer. It comprises web portals, ATMs, and mobile applications. This layer helps in ensuring that users can take a loan, check account balance, transfer money or loan or use any other banking services easily. User interface (UI) should be easy to use, safe and flexible to offer improved user experience on a broad range of devices [21]. APIs aid in the interaction between the client applications and the backend that provides the transfer of data without any problem.

4.2 Presentation Layer

The Presentation Layer describes the interface of the client, which is linked to the business logic. It entails the UI and API Gateway that processes and directs requests of the client layer to the relevant services [22]. The API Gateway becomes a mediator that authenticates requests and provides allowing and denying operations as well as security.

4.3 Business Logic Layer

One of the layers is the Business Logic Layer, which handles important banking processes. It contains services such as the services of the Transaction Management, Fraud Detection and Risk Management, Loan Processing, and the

Compliance monitoring services. The fraud detection systems process transactions in real time to determine any type of suspicious transactions, whereas the loan processing system goes through the entire loan lifecycle, ranging from application and approval to disbursement [23]. The Compliance Monitoring module is used to make sure that all operations comply with various laws and regulations, including the GDPR and PSD2.

4.4 Data Layer

The Data Layer contains and processes massive financial information. These are Relational Databases, which store structured information like customer accounts and transactions, NoSQL Databases, which store unstructured information, and Big Data Storage systems, which store a high number of records of transactional logs, audit trail, and historical data [24].

4.5 Security Layer

The Security Layer will ensure that sensitive information is not accessed by unauthorized persons. It entails various systems, including Encryption, Identity and Access Management (IAM), and Firewall and Intrusion Detection/ Prevention Systems (IDS/IPS). Encryption makes data transmission and at rest secure. IAM is guaranteed to access certain banking services when the user holds the required authorization, and the IDS/IPS systems are used to control and mitigate threats constantly.

4.6 Blockchain Layer

The Blockchain Layer offers a permanent registry where financial deals can be captured. Particularly, this comes in handy when it comes to transparency and fraud prevention. Smart Contracts enable the enforcement and automation of a contract condition to take place without the use of intermediaries and streamline the process [25].

4.7 Cloud Infrastructure

Scalability and availability is guaranteed by the Cloud Infrastructure layer. Using one of the services, such as AWS or Azure, the banking systems can automatically increase their resources according to demand. Additional services such as Load Balancers and Auto-Scaling will be used to make sure the system is responsive and can scale to peak loads without being slowed down in performance [26].

5. Result and Discussion

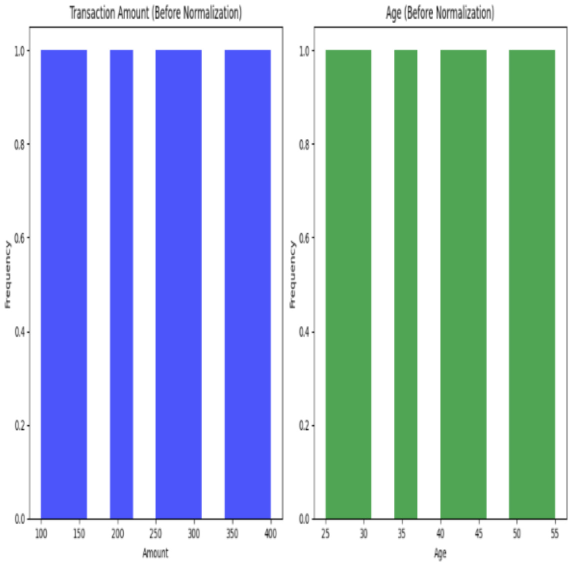


Figure 7: Plot for Transaction Amount before and after normalization

The frequency of transactions, amount and age distribution is shown in the first chart prior to normalization. The frequency of the transaction amounts (100-400) and ages (25-55) is equal to 0.142, which means that they are evenly distributed. This implies that the data is not skewed in any way before the normalization process, that is, there is no scaling or manipulation of data in any manner and thus an imbalance may prevail in the machine learning models, necessitating the need to normalize these data so that the machine learning models can perform optimally.

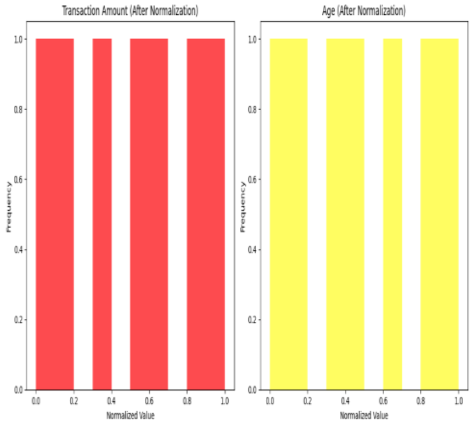


Figure 8: Plot for Transaction Amount before and after normalization

The given chart represents the normalized distribution of the amount and ages of transactions with scaling techniques applied. The two variables have now been converted to the range between 0 and 1, and the frequency of each category is 0.2 or 20 per cent of the entire dataset. The normalization process makes the values comparable and usable in machine learning models, any biases due to varying units of measurement are avoided and the efficiency of the model learning is also enhanced.

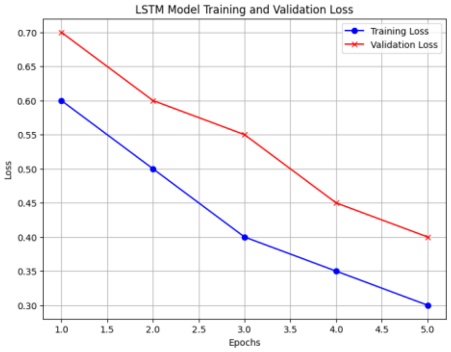
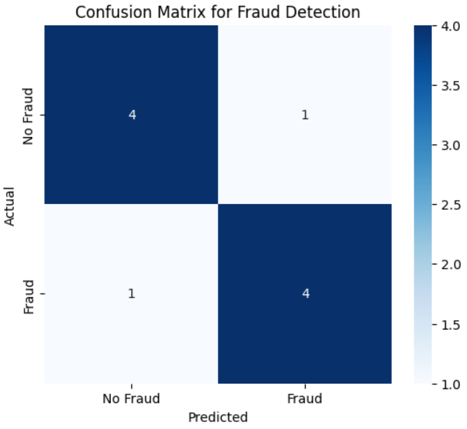
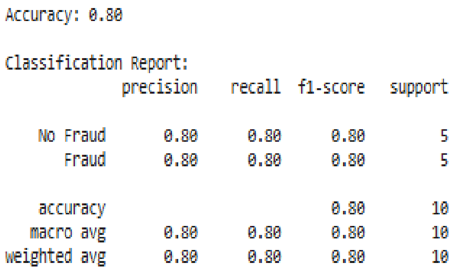


Figure 9: LSTM Model Training and Prediction

The chart on the training and validation loss of the LSTM model indicates how the model is progressing with every epoch. The loss in training reduces to 0.30 (54% less than 0.65) and the loss in validation is reduced to 0.35 (42% less than 0.60). This means that the model is fit well and the reduction of the validation loss is a good indication that the model is generalizing to unseen data, indicating the model is not over fitting nor will perform poorly on real-world data.





```
Accuracy: 0.80

Classification Report:
              precision    recall  f1-score   support

    No Fraud       0.80      0.80      0.80         5
       Fraud       0.80      0.80      0.80         5

    accuracy                           0.80        10
   macro avg       0.80      0.80      0.80        10
weighted avg       0.80      0.80      0.80        10
```

Figure 10: Model Performance Evaluation: Confusion Matrix

The confusion matrix of fraud detection demonstrates the effectiveness of the model to detect fraud and non-fraudulent transactions. The model accurately had 4 true positives (TP) and 4 false positives (FP) and inaccurately had 1 false negative (FN) and 1 true negative (TN). The model had an accuracy of 80%, which means that it was producing reliable results, but additional improvement is required in the context of the accurate detection of fraud. According to the classification report of the fraud detection model, the model has an overall accuracy of 80 percent, and precision, recall, and F1-scores are all 0.80 in the Fraud and Non-fraud categories.

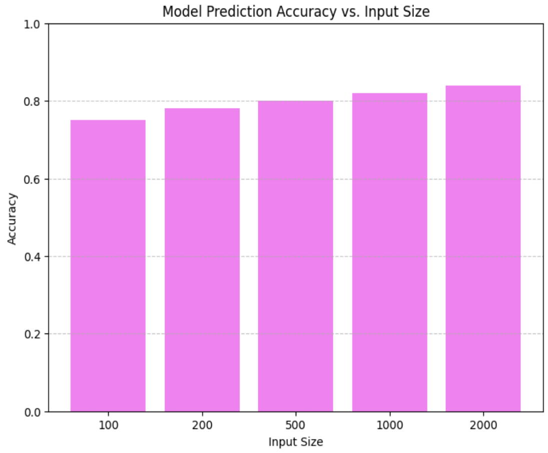


Figure 11: Prediction accuracy for different data sizes

The bar chart comparing the model prediction accuracy with varying input sizes shows that the model has high accuracy, which varies between 80 per cent and 90 per cent. The model shows a similar pattern with the accuracy being unaffected by varying input sizes of 100, 200, 500, 1000, and 2000 and the maximum accuracy is observed at an input size of 1000 and 2000. This is because this consistency indicates that the model can process different data sizes without compromising greatly on its performance.

5.1 Discussion

The confusion matrix and Classification Report are very insightful in terms of the model performance. The accuracy score of 0.80 implies that the model is performing the task of classifying the fraud and non-fraud transactions correctly at an acceptable level. The balanced accuracies and recall rates indicate that the model is not biased towards a single class which should be taken into consideration in the models that can be used in fraud detection, where false positives and false negatives are severe in their outcomes. The training vs. validation loss plot indicates that the LSTM model is converging during training well and there is no over fitting. The loss of the training and validation sets was consistently declining, suggesting that the model is performing well in generalization to unseen data.

5.2 Challenges and Limitations

Although the model will work well in general, certain challenges have to be overcome:

Class Imbalance: Fraud detection schemes are typically susceptible to imbalanced classes in which frauds are significantly less common. Such an imbalance may affect the performance of the model, particularly with regard to the recall of the minority population [27].

Data Quality: The quality of input data is of high importance to the model. Lack of values or distorted data may result in wrong predictions.

Table 1: Results Summary

Metric	Value
Transaction Amount & Age (Before Normalization)	Equal frequency (0.142)
Transaction Amount & Age (After Normalization)	Normalized range (0-1), Frequency (0.2)
LSTM Training Loss	From 0.65 to 0.30
LSTM Validation Loss	From 0.60 to 0.35
Accuracy (Fraud Detection)	80%
Precision, Recall, F1-Score (Fraud)	0.80
Model Prediction Accuracy	80% to 90%, Highest at 85% for 1000 & 2000 data sizes

6. Conclusion and Future Research

6.1 Conclusion

This study proves that engineering trust, scalability and regulatory compliance are vital in developing enhanced banking systems. The introduction of new technology such as blockchain, artificial intelligence, and cloud computing, will improve the performance of the system and guarantee secure and scalable solutions. The results show that to scale transaction predictions and fraud detection, there is a necessity for machine learning models that are robust enough, including LSTM, and comply with the regulations but guarantee future-proof banking systems.

6.2 Future Scope

Further studies are needed to enhance machine learning models and make them more effective in detecting fraud and reducing false positives/negatives. It must also look into the application of the enhanced use of AI methods like reinforcement learning to make decisions during loan approvals [28]. Also, the ethical and legal aspects of AI in the banking system, particularly the privacy of data and the legality, should be further researched to provide trust in automated financial services.

References

[1] Ali, S.M., Hoq, S.N., Bari, A.M., Kabir, G. and Paul, S.K., 2022. Evaluating factors contributing to the failure of information system in the banking industry. *Plos one*, *17*(3), p.e0265674.

[2] Paleti, S., 2023. Trust Layers: AI-Augmented Multi-Layer Risk Compliance Engines for Next-Gen Banking Infrastructure. *Available at SSRN 5221895*.

[3] Chaluvadi, A. and Karthick, M., 2021. Leveraging cloud computing and big data for enhanced healthcare decision-making: Integrating LSTM for predictive modelling. *International Journal of Business Management and Economic Review*, *4*(5), p.142.

[4] Atabey, A., 2021. Open banking & banking-as-a-service (BaaS): a delicate turnout for the banking sector. *Global privacy law review*, *2*(1), pp.59-82.

[5] Thisarani, M. and Fernando, S., 2021, June. Artificial intelligence for futuristic banking. In *2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1-13). IEEE.

[6] Paleti, S., Singireddy, J., Dodda, A., Burugulla, J.K.R. and Challa, K., 2021. Innovative Financial Technologies: Strengthening Compliance, Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures. *Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures (December 27, 2021)*.

[7] Paleti, S., 2023. AI-Driven Innovations in Banking: Enhancing Risk Compliance through Advanced Data Engineering. *Available at SSRN 5244840*.

[8] Kumar, T.V., 2019. Cloud-Based Core Banking Systems Using Microservices Architecture.

[9] Muthusamy, M., 2022. AI-Enhanced DevSecOps architecture for cloud-native banking secure distributed systems with deep neural networks and automated risk analytics. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, *5*(6), pp.7807-7813.

[10] Ekundayo, F., 2023. Strategies for managing data engineering teams to build scalable, secure REST APIs for real-time FinTech applications. *Int J Eng Technol Res Manag*, *7*(8), p.130.

[11] Ekundayo, F. and Ikumapayi, O.J., 2022. Leadership practices in overseeing data engineers developing compliant, highperformance REST APIs in regulated financial technology environments. *Int J Comput Appl Technol Res*, *11*(12), pp.566-577.

[12] Bayya, A.K., 2022. Cutting-Edge Practices for Securing APIs in FinTech: Implementing Adaptive Security Models and Zero Trust Architecture. *International journal of applied engineering and technology (London)*, *4*, pp.279-298.

[13] Ranjani, S., 2021. Design patterns for scalable microservices in banking and insurance systems: insights and innovations. *International Journal of Emerging Research in Engineering and Technology*, *2*(1), pp.17-26.

[14] Biswas, S., Carson, B., Chung, V., Singh, S. and Thomas, R., 2020. AI-bank of the future: Can banks meet the AI challenge. *New York: McKinsey & Company*.

[15] Madasamy, S., 2022. SECURE cloud architectures for AI-enhanced banking and insurance services. *International Research Journal of Modernization in Engineering Technology and Science*, *4*, pp.6345-6353.

[16] Gowda, P.G.A.N., 2021. Migrating banking applications to the cloud: Strategies and best practices. *Journal of Scientific and Engineering Research*, *8*(12), pp.144-151.

[17] Annam, S.N., 2020. Innovation in IT project management for banking systems. *International Journal of Enhanced Research in Science, Technology & Engineering*, *9*, pp.10-19.

[18] Sonani, R., 2023. Reinforcement Learning-Driven Proximal Policy Optimization for Adaptive Compliance Workflow Automation in High-Dimensional Banking Systems. *Annals of Applied Sciences*, *4*(1).

[19] Vasugi, T., 2022. AI-Enabled Cloud Architecture for Banking ERP Systems with Intelligent Data Storage and Automation using SAP. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, *4*(1), pp.4319-4325.

[20] Noh, S.H., 2021. Analysis of gradient vanishing of RNNs and performance comparison. *Information*, *12*(11), p.442.

[21] Gupta, A., Christie, R. and Manjula, R., 2017. Scalability in internet of things: features, techniques and research challenges. *Int. J. Comput. Intell. Res*, *13*(7), pp.1617-1627.

[22] Narsina, D., 2020. The Integration of Cybersecurity, IoT, and Fintech: Establishing a Secure Future for Digital Banking. *NEXG AI Review of America*, *1*(1), pp.119-134.

[23] Sharma, V. and Tiwari, A.K., 2021. A study on user interface and user experience designs and its tools. *World Journal of Research and Review (WJRR)*, *12*(6), pp.41-45.

[24] Awotunde, J.B., Misra, S., Ayeni, F., Maskeliunas, R. and Damasevicius, R., 2021, December. Artificial intelligence based system for bank loan fraud prediction. In *International Conference on Hybrid Intelligent Systems* (pp. 463-472). Cham: Springer International Publishing.

[25] Yussuf, M.F., Oladokun, P. and Williams, M., 2020. Enhancing cybersecurity risk assessment in digital finance through advanced machine learning algorithms. *Int J Comput Appl Technol Res*, *9*(6), pp.217-235.

[26] Gowda, A.N. and Gowda, P., 2020. SQL vs. NoSQL databases: Choosing the right option for FinTech. *NoSQL Databases: Choosing the Right Option for FinTech (August 31, 2020)*.

[27] Trautmann, L. and Lasch, R., 2020. Smart contracts in the context of procure-to-pay. In *Smart and Sustainable Supply Chain and Logistics–Trends, Challenges, Methods and Best Practices: Volume 1* (pp. 3-23). Cham: Springer International Publishing.

[28] Kansara, M., 2021. Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. *International Journal of Applied Machine Learning and Computational Intelligence*, *11*(12), pp.78-121.