International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Financial Fraud Detection in Banking Systems: Integrating IoT, Deep Learning, and Big Data Analytics for Real-time Security

Dr. B R Celia[1], Dr. Shahanawaj Ahamad[2,*], Manisha Mittal[3], Elangovan Muniyandy[4], Aruna Kolukulapalli[5], Amit Verma[6], Dharmesh Dhabliya[7]

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: Financial fraud poses a significant threat to banking systems, with increasingly sophisticated attacks targeting sensitive customer data and financial transactions. This paper proposes an innovative approach to enhance financial fraud detection in banking systems by integrating Internet of Things (IoT), deep learning, and big data analytics for real-time security. By leveraging IoT devices to gather real-time transaction data and user behavior patterns, coupled with advanced deep learning algorithms and big data analytics techniques, banks can detect and prevent fraudulent activities more effectively. This paper outlines the key principles and mechanisms underlying the integration of IoT, deep learning, and big data analytics in financial fraud detection. Furthermore, it discusses the potential benefits and challenges of adopting this approach, as well as future research directions to improve real-time security in banking systems.

Keywords: *Financial Fraud Detection, Banking system, IoT, Deep learning, Big Data Analytics, Real time security*

1. Introduction

In recent years, financial fraud has become a pervasive and sophisticated threat to banking systems worldwide. With the rise of digital banking and online transactions, fraudsters have evolved their tactics to exploit vulnerabilities in traditional security measures, resulting in significant financial losses and reputational damage for financial institutions. In response to these challenges, there is a growing need for innovative approaches to enhance financial fraud detection in banking systems. This paper proposes a novel approach to address the shortcomings of existing fraud detection mechanisms by integrating Internet of Things (IoT), deep learning, and big data analytics for real-time security. By harnessing the power of IoT devices, which capture real-time transaction data and user behavior patterns, coupled with advanced deep learning algorithms and big data analytics techniques, banks can achieve more effective and proactive detection of fraudulent activities.

The integration of IoT, deep learning, and big data analytics offers several advantages for financial fraud detection in banking systems. Firstly, IoT devices, such as sensors and wearables, enable the collection of rich and diverse data streams, including transaction history, biometric data, and geolocation information, which can be used to detect anomalies and patterns indicative of fraudulent behavior. Secondly, deep learning algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), provide advanced capabilities for feature extraction, pattern recognition, and anomaly detection in large-scale datasets. Finally, big data analytics techniques, such as stream processing, distributed computing, and real-time analytics, enable banks to analyze and respond to fraud events in real-time, minimizing the impact of fraudulent activities on customers and the financial institution. In this paper, we will explore the key principles and mechanisms underlying the integration of IoT, deep learning, and big data analytics in financial fraud detection. We will discuss the potential benefits of adopting this approach, including improved detection accuracy, reduced false positives, and enhanced real-time security. Furthermore, we will examine the challenges and limitations associated with implementing IoT, deep learning, and big data analytics in banking systems, such as data privacy concerns, scalability issues, and computational complexity. Overall, the integration of IoT, deep learning, and big data analytics represents a promising avenue for enhancing financial fraud detection in banking systems. By leveraging the synergies between these technologies, financial institutions can strengthen their defences against fraudulent activities, safeguard customer assets, and preserve trust in the digital banking ecosystem.

[1]Professor, Department of Commerce CS, Saveetha College of Liberal Arts and Sciences, Saveetha Institute of Medical and Technical Sciences, Thandalam-602105, Tamil Nadu, India Email: celiajaidhas@gmail.com
[2]Associate Professor, Department of Software Engineering, College of Computer Science and Engineering, University of Hail, Hail City, Saudi Arabia Email: drshahwj@gmail.com
[3]Associate Professor, Department of Electronics and Communication Engineering, Guru Tegh Bahadur Institute of Technology, GGSIPU, New Delhi, India Email: manumanisha22@gmail.com
[4]Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India Email: muniyandy.e@gmail.com
[5]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India Email: karuna@kluniversity.in
[6]University Centre for Research and Development, Chandigarh University, Gharuan Mohali, Punjab, India Email: amit.e9679@cumail.in
[7]Professor, Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India Email: dharmesh.dhabliya@viit.ac.in
[*]Corresponding Author: - Dr. Shahanawaj Ahamad (drshahwj@gmail.com)

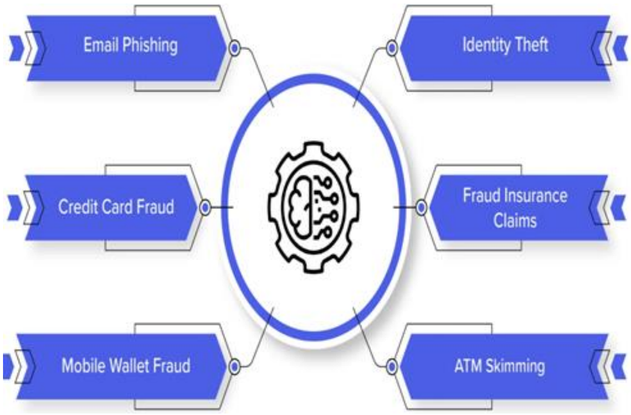

Fig 1. Financial Fraud Detection System [13]

2. Existing research

This section reviews the literature on credit card and internet banking fraud detection techniques. Based on credit card and online banking fraud detection methods, these research publications are chosen and reviewed from recent years.

Abdullah Alharbi and colleagues (2022) used the Kaggle dataset to construct a deep learning (DL) solution for text data. An novel approach for turning text to visuals produces little graphics. The photos were input into the CNN architecture with class weights using the inverse frequency technique to fix class imbalance. Deep learning and machine learning were utilized to verify the proposed system [1]. A fraud detection system model by Xinwei Zhang and colleagues (2021) uses a deep learning architecture and an upgraded feature engineering technique based on Homogeneity-Oriented Behavior Analysis. The framework's efficiency was assessed by comparison [2]. An actual dataset from a big Chinese commercial bank was used for the investigation. Huang Tingfei and colleagues (2020) use variational automated coding (VAE) and deep learning to solve this problem by oversampling. A large number of minority group instances were created using VAE in an uneven dataset. The classification network was trained using these instances [3]. JavadForough and SaeedehMomtazi (2022) developed a novel model to detect net banking and credit card fraud using sequence labeling, deep neural networks, and Probabilistic Graphical Models (PGM). Our model was then compared against the baseline model using two real-world datasets. We also examined how hidden sequential links among transactions and anticipated labels may improve results. A novel undersampling method preserves sequential data patterns during random undersampling [4]. Ebenezer Esenoghoet al. (2022) employ a neural network ensemble classifier with hybrid data resampling to identify credit card and online banking fraud. The ensemble classifier was created using adaptive boosting (AdaBoost) and an LSTM neural network as the basis learner. Hybrid resampling was done using synthetic minority oversampling and modified closest neighbor (SMOTE-ENN) at this period. The method was validated using public Netbanking and credit card transaction datasets [5]. The revolutionary Neural Aggregate Generator (NAG) neural network-based feature extraction module learns feature aggregates end-to-end for fraud categorization. Dastidar and colleagues (2022) defined this module. Unlike earlier automated feature extraction approaches, the NAG's network topology closely resembles feature aggregates. A soft feature value matching and relative weighting of feature constraints allow the NAG to extend learnable aggregates beyond conventional ones [6]. V. S. S. Karthik and colleagues (2021) develop a novel model for detecting online banking and credit card fraud. This model uses ensemble learning methods like boosting and bagging. Our hybrid model uses bagging and boosting ensemble classifiers to encompass the best of both techniques [7]. AltyebAltaherTaha and SharafJameelMalebary (2020) created an innovative approach for detecting Netbanking and credit card fraud. This approach uses an OLightGBM, or optimized light gradient boosting machine. Intelligently integrating a Bayesian-based hyper-parameter optimization approach to tune light gradient boosting machine (LightGBM) parameters is offered [8]. Benchaji et al. (2021) develop an online banking and credit card fraud detection system. To incorporate transaction sequences, this system uses LSTM networks as sequence learners. The created method records credit card and Netbanking users' past purchasing activity to enhance fraud detection on fresh incoming transactions. In experiments, our model yields robust findings with excellent accuracy [9]. Zorion (2023) studied credit card fraud detection. Deep Learning was investigated for this [41,10]. R. Achary (2023) studied banking fraud detection. They considered machine learning [42,11].

3. Problem statement

While integrating IoT, deep learning, and big data analytics offers promising avenues for enhancing financial fraud detection in banking systems, there are several limitations and challenges that need to be addressed:

1. Data Quality and Availability: IoT devices generate vast amounts of data, but the quality and reliability of this data can vary. Inaccurate or incomplete data from IoT sensors can lead to false alarms and misclassifications in fraud detection systems. Additionally, accessing and integrating data from disparate sources within banking systems may pose challenges due to data silos and compatibility issues.

2. Privacy and Regulatory Compliance: Collecting and analyzing sensitive financial data from IoT devices raises privacy concerns and regulatory compliance challenges. Financial institutions must ensure compliance with data protection laws (e.g., GDPR, CCPA) and industry regulations (e.g., PCI DSS) while maintaining the confidentiality and integrity of customer information. Balancing the need for data security with regulatory requirements can be a complex and delicate task.

3. Scalability and Performance: Processing and analyzing large volumes of IoT data in real-time requires scalable infrastructure and high-performance computing resources. Deep learning models, in particular, can be computationally intensive and may require significant resources for training and inference. Ensuring scalability and performance while maintaining low latency is crucial for effective real-time fraud detection in banking systems.

4. Model Interpretability and Explainability: Deep learning models are often considered black-boxes, making it challenging to interpret their decisions and understand the underlying factors contributing to fraud detection. Lack of model interpretability and explainability may hinder trust and adoption among stakeholders, including bank regulators, auditors, and customers. Developing techniques for explaining and visualizing deep

learning models' decisions is essential for improving transparency and accountability in fraud detection systems.

5. Adversarial Attacks and Security Vulnerabilities: Deep learning models are susceptible to adversarial attacks, where malicious actors manipulate input data to deceive the model and evade detection. Adversarial attacks targeting financial fraud detection systems can lead to false negatives and undetected fraud instances, undermining the system's effectiveness and reliability. Enhancing robustness and resilience against adversarial attacks is critical for ensuring the security and integrity of fraud detection systems.

6. Cost and Resource Constraints: Implementing and maintaining an integrated IoT, deep learning, and big data analytics infrastructure requires significant investment in technology, expertise, and resources. Small and medium-sized financial institutions may face challenges in deploying and managing such complex systems, particularly in terms of budget constraints and talent shortages. Finding cost-effective solutions that balance performance, scalability, and affordability is essential for widespread adoption.

7. Human Oversight and Decision-making: While automated fraud detection systems can improve efficiency and scalability, human oversight and decision-making remain crucial for verifying alerts, investigating suspicious activities, and making informed decisions. Overreliance on automated systems without human intervention may increase the risk of false positives and false negatives, leading to missed opportunities or unnecessary disruptions for legitimate transactions.

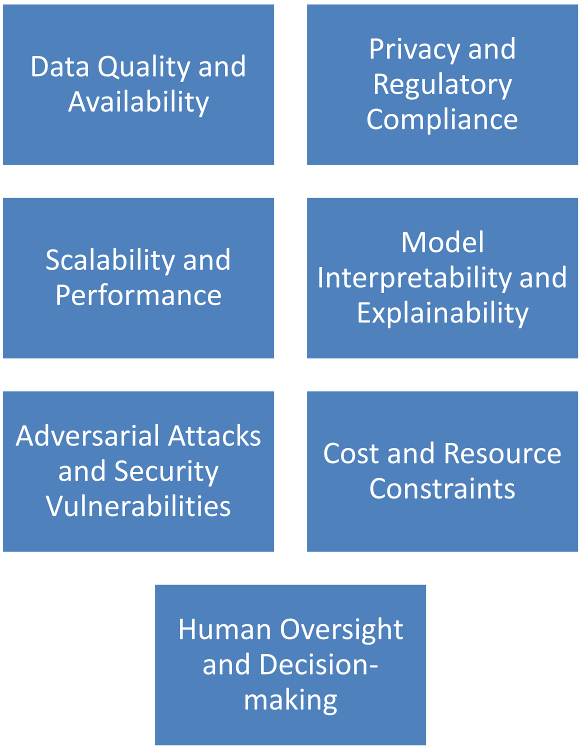
Data Quality and Availability
Privacy and Regulatory Compliance
Scalability and Performance
Model Interpretability and Explainability
Adversarial Attacks and Security Vulnerabilities
Cost and Resource Constraints
Human Oversight and Decision-making

Fig 2 Issues with Financial Fraud Detection system

Addressing these limitations requires a multidisciplinary approach that integrates expertise in data science, cybersecurity, regulatory compliance, and risk management. Collaboration between financial institutions, technology vendors, regulators, and researchers is essential for developing effective and sustainable solutions for enhancing financial fraud detection in banking systems.

4. Need of research

The need for enhancing financial fraud detection in banking systems through the integration of IoT, deep learning, and big data analytics for real-time security is driven by several key factors:

1. Rising Instances of Financial Fraud: Financial fraud, including payment card fraud, identity theft, and account takeover, continues to increase in frequency and sophistication, posing significant risks to banks and their customers. Traditional fraud detection methods are often reactive and unable to keep pace with evolving fraud schemes, highlighting the need for more advanced and proactive detection mechanisms.

2. Complexity of Fraudulent Activities: Fraudsters employ sophisticated techniques to circumvent traditional security measures, such as spoofing, phishing, and social engineering attacks. These techniques exploit vulnerabilities in banking systems and leverage advanced technologies, making it challenging for banks to detect and prevent fraudulent activities using conventional methods alone.

3. Real-time Security Requirements: In today's fast-paced digital economy, real-time security is essential for safeguarding financial transactions and protecting customer assets. Delayed detection of fraudulent activities can result in substantial financial losses and reputational damage for banks, highlighting the importance of real-time monitoring and response capabilities in fraud detection systems.

4. Volume and Velocity of Data: The proliferation of digital channels and IoT devices has led to an exponential increase in the volume and velocity of data generated by banking systems. Traditional fraud detection systems struggle to process and analyze this vast amount of data in real-time, necessitating the use of advanced analytics techniques, such as deep learning and big data analytics, to extract actionable insights and identify fraudulent patterns.

5. Regulatory Compliance Requirements: Regulatory authorities impose stringent requirements on banks to implement effective fraud detection and prevention measures to protect customer data and ensure compliance with industry standards and regulations. Failure to detect and mitigate fraudulent activities can result in severe penalties, fines, and legal consequences for banks, underscoring the importance of investing in robust fraud detection solutions.

6. Customer Trust and Confidence: Financial fraud erodes customer trust and confidence in banking institutions, leading to customer churn, negative publicity, and reputational damage. By enhancing fraud detection capabilities and ensuring the security of customer transactions, banks can foster trust and loyalty among their customers, thereby maintaining their competitive edge in the market.

Need for enhancing financial fraud detection in banking systems through the integration of IoT, deep learning, and big data analytics for real-time security is driven by the increasing frequency and complexity of fraudulent activities, the imperative for real-time security in digital transactions, the volume and velocity of data generated by banking systems, regulatory compliance requirements, and the importance of maintaining customer trust and confidence. By leveraging advanced technologies and analytics techniques, banks can strengthen their fraud detection capabilities, mitigate risks, and protect customer assets in an increasingly digital and interconnected world.

5. Proposed work

The process flow of enhancing financial fraud detection in banking systems through the integration of IoT, deep learning, and big data analytics for real-time security involves several key steps:

1. Data Collection from IoT Devices:
 - IoT devices such as sensors, wearables, and mobile devices are deployed to collect real-time transaction data, user behavior patterns, and contextual information.
 - Transactional data includes information such as transaction amounts, timestamps, locations, and user interactions, which are captured by IoT sensors and devices connected to banking systems.

2. Data Preprocessing and Feature Engineering:
 - Raw data collected from IoT devices undergo preprocessing steps to clean, normalize, and transform the data into a suitable format for analysis.
 - Feature engineering techniques are applied to extract relevant features and variables from the raw data, such as transaction frequency, transaction amounts, geographic locations, and user demographics.

3. Deep Learning Model Training:
 - Deep learning algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are trained on the preprocessed data to learn patterns and relationships indicative of fraudulent activities.
 - Training data includes labeled examples of fraudulent and legitimate transactions, allowing the deep learning models to learn to distinguish between normal and anomalous behavior.

4. Model Validation and Evaluation:
 - The trained deep learning models are validated and evaluated using validation datasets to assess their performance in detecting fraudulent activities.
 - Evaluation metrics such as accuracy, precision, recall, and F1 score are computed to measure the model's effectiveness in identifying fraudulent transactions while minimizing false positives and false negatives.

5. Real-time Fraud Detection:
 - The validated deep learning models are deployed in real-time fraud detection systems to analyze incoming transaction data and detect fraudulent activities.
 - Real-time analytics platforms and stream processing frameworks are used to process and analyze transaction data in real-time, enabling immediate detection and response to fraudulent events.

6. Anomaly Detection and Alert Generation:
 - Deep learning models identify anomalies and suspicious patterns in transaction data based on learned patterns and thresholds.
 - When a potential fraud event is detected, alerts are generated and sent to fraud analysts or automated systems for further investigation and action.

7. Fraud Investigation and Response:
 - Upon receiving alerts, fraud analysts investigate the flagged transactions to determine their legitimacy and severity.
 - Depending on the outcome of the investigation, appropriate actions are taken, such as blocking suspicious transactions, freezing accounts, and initiating fraud investigations.

8. Model Updating and Iteration:
 - The performance of the deep learning models is continuously monitored and evaluated over time.
 - Models are updated and retrained periodically using new data to adapt to evolving fraud patterns and maintain high detection accuracy.

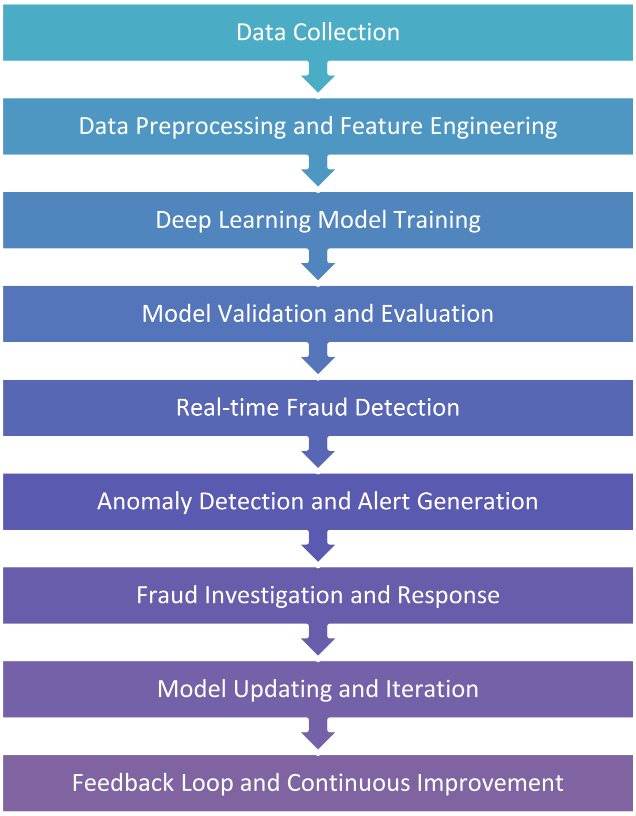
Data Collection
Data Preprocessing and Feature Engineering
Deep Learning Model Training
Model Validation and Evaluation
Real-time Fraud Detection
Anomaly Detection and Alert Generation
Fraud Investigation and Response
Model Updating and Iteration
Feedback Loop and Continuous Improvement

Fig 3. Model for crop monitoring

9. Feedback Loop and Continuous Improvement:
 - Feedback from fraud analysts and system users is collected to identify areas for improvement and refinement in the fraud detection system.
 - Continuous improvement efforts focus on optimizing model performance, reducing false positives, and enhancing the overall effectiveness of the fraud detection system.

By following this process flow, banks can enhance their financial fraud detection capabilities through the integration of

IoT, deep learning, and big data analytics for real-time security, enabling proactive detection and mitigation of fraudulent activities in banking systems.

6. Simulation Results

Dataset of fraud activity has been captured from kaggle.com. Simulation has been made using deep learning for fraud activity detection..

6.1. Fraud detection accuracy

Confusion matrix obtained in the case of previous research is shown in Table 1.

Table 1. Previous work Confusion matrix

	Fraud	**Normal**
Fraud	5773	225
Normal	227	5775

Table 2 is presenting confusion matrix in case of proposed work.

Table 2. Proposed work Confusion matrix

	Fraud	**Normal**
Fraud	5893	105
Normal	107	5895

6.2. Accuracy Comparison

Table 3 is showing the comparative analysis of accuracy parameters in case of conventional and proposed work.

Table 3. Accuracy in case of proposed model

Measure	**Previous**	**Proposed**
Accuracy	0.9623	0.9823
Precision	0.9625	0.9825
F1 Score	0.9623	0.9823

Taking into consideration table 3, figure 4 provides a graphical depiction of the average accuracy parameters in the case of both the proposed model and the prior model.

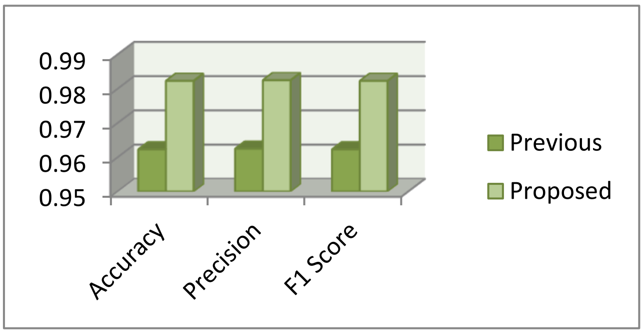

Fig. 4. Comparison of previous and proposed work considering accuracy parameters

Sensitivity and specificity of previous and proposed approach has been shown in table 4

Table 4. Comparison of sensitivity and specificity

Measure	Previous	Proposed
Sensitivity	0.9622	0.9822
Specificity	0.9625	0.9825

Considering table 4, there is graphical representation of sensitivity and specific for proposed and previous model is shown in figure 5.

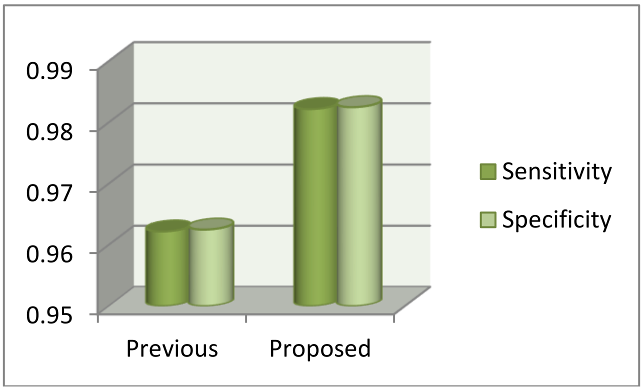

Fig. 5. Comparison of specificity and sensitivity of previous and proposed work

7. Conclusion

In conclusion, the integration of Internet of Things (IoT), deep learning, and big data analytics presents a promising approach to enhancing financial fraud detection in banking systems, enabling real-time security and proactive risk mitigation. This paper has explored the principles, challenges, and future scope of integrating these advanced technologies to combat the evolving threat landscape of financial fraud.

1. Benefits of Integration: By leveraging IoT devices to gather real-time transaction data, deep learning algorithms for pattern recognition, and big data analytics for real-time analysis, banks can achieve more effective and proactive detection of fraudulent activities. This integration enables financial institutions to detect anomalies, identify suspicious patterns, and respond to fraud events in real-time, minimizing the impact on customers and the organization.

2. Advancements in Deep Learning: Continued advancements in deep learning techniques, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and attention mechanisms, offer opportunities to improve the accuracy and efficiency of financial fraud detection models. These techniques enable banks to extract meaningful insights from large-scale transaction data and identify fraudulent behavior with higher precision and recall rates.

3. Real-time Security and Response: The integration of IoT, deep learning, and big data analytics enables banks to detect and respond to fraud events in real-time, reducing the window of opportunity for fraudsters to exploit vulnerabilities. By leveraging real-time analytics and automated decision-making, financial institutions can take immediate action to block fraudulent transactions, alert customers, and initiate fraud investigations, enhancing overall security posture.

4. Challenges and Considerations: Despite the potential benefits, integrating IoT, deep learning, and big data analytics poses several challenges, including data quality and availability, privacy concerns, scalability issues, and regulatory compliance requirements. Addressing these challenges requires a multidisciplinary approach that integrates expertise in data science, cyber security, regulatory compliance, and risk management.

5. Future Directions: The future scope of enhancing financial fraud detection through IoT, deep learning, and big data analytics is characterized by ongoing innovation, collaboration, and convergence of technologies.

The integration of IoT, deep learning, and big data analytics represents a promising approach to enhancing financial fraud detection in banking systems, enabling real-time security and proactive risk mitigation. By leveraging the synergies between these advanced technologies and addressing the associated challenges, financial institutions can strengthen their defenses against fraudulent activities, safeguard customer assets, and preserve trust in the banking ecosystem.

8. Future Scope

The future scope of enhancing financial fraud detection in banking systems through the integration of IoT, deep learning, and big data analytics for real-time security is promising and encompasses several areas of development and innovation:

1. Advanced Deep Learning Techniques: Continued advancements in deep learning algorithms, such as graph neural networks, reinforcement learning, and generative adversarial networks, hold promise for improving the accuracy and effectiveness of financial fraud detection systems. These techniques can better capture complex patterns and relationships in large-scale financial transaction data, leading to more robust and adaptive fraud detection models.

2. Explainable AI and Model Interpretability: Addressing the interpretability challenge of deep learning models is crucial for enhancing trust and transparency in financial fraud detection systems. Future research will focus on developing explainable AI techniques and model interpretability methods to provide insights into the decision-making process of deep learning models, enabling stakeholders to understand and validate model predictions.

3. Privacy-Preserving Technologies: Innovations in privacy-preserving technologies, such as federated learning, differential privacy, and secure multiparty computation, will enable financial institutions to analyze sensitive transaction data while protecting customer privacy and complying with regulatory requirements. These technologies allow collaborative model training across distributed data sources without sharing raw data, mitigating privacy risks and ensuring data confidentiality.

4. Blockchain and Distributed Ledger Technology: Integration of blockchain and distributed ledger technology (DLT) with financial fraud detection systems can enhance data integrity, traceability, and auditability in banking transactions. Blockchain-enabled smart contracts can automate fraud detection processes, enforce compliance rules, and facilitate secure data sharing among financial institutions, regulators, and law enforcement agencies, reducing fraud-related risks and improving regulatory oversight.

5. Edge Computing and IoT Devices: Leveraging edge computing and IoT devices for real-time data processing and analysis at the network edge can enhance the responsiveness and scalability of financial fraud detection systems. Edge-based analytics can enable faster detection and mitigation of fraudulent activities, reducing the reliance on centralized data processing and improving system resilience to network disruptions and cyber attacks.

6. Quantum Computing: The advent of quantum computing holds promise for revolutionizing financial fraud detection through quantum-resistant cryptographic algorithms and quantum-enhanced machine learning techniques. Quantum computing can enable faster and more efficient processing of large-scale financial datasets, enabling banks to detect and respond to fraud in real-time with unprecedented speed and accuracy.

7. Collaborative Threat Intelligence Sharing: Establishing collaborative platforms for threat intelligence sharing among financial institutions, regulatory agencies, and cybersecurity vendors can enhance situational awareness and collective defense against evolving fraud threats. Real-time exchange of threat intelligence data, including indicators of compromise (IOCs) and behavioral analytics insights, can enable proactive detection and mitigation of fraud schemes across the banking ecosystem.

8. Continuous Monitoring and Adaptive Security: Implementing continuous monitoring and adaptive security measures, such as anomaly detection, behavioral analytics, and real-time risk scoring, will enable financial institutions to detect emerging fraud patterns and adapt their defenses accordingly. Machine learning-driven adaptive security systems can learn from historical fraud incidents and dynamically adjust their detection algorithms to stay ahead of evolving threats.

The future scope of enhancing financial fraud detection in banking systems through the integration of IoT, deep learning, and big data analytics for real-time security is characterized by ongoing innovation, collaboration, and convergence of technologies. By leveraging the synergies between these advanced technologies, financial institutions can strengthen their fraud detection capabilities, safeguard customer assets, and preserve trust in the banking ecosystem...

References

[1] Alharbi, A., Alshammari, M., Okon, O.D., Alabrah, A., Rauf, H.T., Alyami, H. and Meraj, T., “A Novel text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning”, Approach. Electronics, vol.11, no.5, pp.756, March 2022.

[2] Zhang, X., Han, Y., Xu, W. and Wang, Q., “HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture”, Information Sciences, vol.557, pp.302-316, May 2021.

[3] Tingfei, H., Guangquan, C. and Kuihua, H., “Using variational auto encoding in credit card fraud detection”, IEEE Access, vol.8, pp.149841-149853, August 2020.

[4] Forough, J. and Momtazi, S., “Sequential credit card fraud detection: A joint deep neural network and probabilistic graphical model approach”, Expert Systems, vol.39, no.1, pp.e12795, January 2022.

[5] Esenogho, E., Mienye, I.D., Swart, T.G., Aruleba, K. and Obaido, G., “A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection”, IEEE Access, vol.10, pp.16400-16407, January 2022.

[6] Dastidar, K.G., Jurgovsky, J., Siblini, W., He-Guelton, L. and Granitzer, M., “NAG: Neural feature aggregation framework for credit card fraud detection”, Knowledge and Information Systems, vol.64, pp.831–858, February 2022.

[7] Karthik, V.S.S., Mishra, A. and Reddy, U.S., “Credit Card Fraud Detection by Modelling Behaviour Pattern using Hybrid Ensemble Model”, Arabian Journal for Science and Engineering, pp.1-11, September 2021.

[8] Taha, A.A. and Malebary, S.J., “An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine”, IEEE Access, vol.8, pp.25579-25587, February 2020.

[9] Datta, P., Panda, S.N., Tanwar, S. and Kaushal, R.K., “A technical review report on cyber crimes in India”, In proceedings of 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), pp.269-275, March 2020.

[10] Boddu, R.S.K. and Bendi, V.R., “Cyber Crime and Security, a Global Vulnerable Coercion: Obstacles and Remedies”, International Journal of Information and Electronics Engineering, vol.7, no.5, September 2017.

[11] Randhawa, K., Loo, C.K., Seera, M., Lim, C.P. and Nandi, A.K., “Credit card fraud detection using AdaBoost and majority voting”, IEEE access, vol.6, pp.14277-14284, February 2018..

[12] A. Gupta, D. Kaushik, M. Garg and A. Verma, "Machine Learning model for Breast Cancer Prediction," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 472-477, doi: 10.1109/I-SMAC49090.2020.9243323

[13] https://appinventiv.com/wp-content/uploads/sites/1/2021/12/How-Machine-Learning-Helps-in-Financial-Fraud-Detection-in-the-FinTech-Industry_Info-1-10-scaled.webp

[14] V. Veeraiah, K. R. Kumar, P. Lalitha Kumari, S. Ahamad, R. Bansal and A. Gupta, "Application of Biometric System to Enhance the Security in Virtual World," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 719-723, doi: 10.1109/ICACITE53722.2022.9823850.

[15] V. Veeraiah, G. P, S. Ahamad, S. B. Talukdar, A. Gupta and V. Talukdar, "Enhancement of Meta Verse Capabilities by IoT Integration," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1493-1498, doi: 10.1109/ICACITE53722.2022.9823766.

[16] Kaushik Dushyant; Garg Muskan; Annu; Ankur Gupta; Sabyasachi Pramanik, "Utilizing Machine Learning and Deep Learning in Cybesecurity: An Innovative Approach," in Cyber Security and Digital Forensics: Challenges and Future Trends , Wiley, 2022, pp.271-293, doi: 10.1002/9781119795667.ch12.

[17] V. Veeraiah, H. Khan, A. Kumar, S. Ahamad, A. Mahajan and A. Gupta, "Integration of PSO and Deep Learning for Trend Analysis of Meta-Verse," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 713-718, doi: 10.1109/ICACITE53722.2022.9823883.

[18] V. Talukdar, D. Dhabliya, B. Kumar, S. B. Talukdar, S. Ahamad and A. Gupta, "Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.

[19] V. Jain, S. M. Beram, V. Talukdar, T. Patil, D. Dhabliya and A. Gupta, "Accuracy Enhancement in Machine Learning During Blockchain Based Transaction Classification," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 536-540, doi: 10.1109/PDGC56933.2022.10053213.

[20] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Comparative study of 4G, 5G and 6G Networks," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1830-1833, doi: 10.1109/IC3I56241.2022.10073385.

[21] P. Venkateshwari, V. Veeraiah, V. Talukdar, D. N. Gupta, R. Anand and A. Gupta, "Smart City Technical Planning Based on Time Series Forecasting of IOT Data," 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), Ghaziabad, India, 2023, pp. 646-651, doi: 10.1109/ICSEIET58677.2023.10303480.

[22] V. Veeraiah, J. Kotti, V. Jain, T. Sharma, S. Saini and A. Gupta, "Scope of IoT in Emerging Engineering Technology during Online Education," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308107.

[23] Bijender Bansal; V. Nisha Jenipher; Rituraj Jain; R. Dilip; Makhan Kumbhkar; Sabyasachi Pramanik; Sandip Roy; Ankur Gupta, "Big Data Architecture for Network Security," in Cyber Security and Network Security , Wiley, 2022, pp.233-267, doi: 10.1002/9781119812555.ch11.

[24] K. A. Shukla, S. Almal, A. Gupta, R. Jain, R. Mishra and D. Dhabliya, "DL Based System for On-Board Image Classification in Real Time, Applied to Disaster Mitigation," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 663-668, doi: 10.1109/PDGC56933.2022.10053139.

[25] R. Bansal, A. Gupta, R. Singh and V. K. Nassa, "Role and Impact of Digital Technologies in E-Learning amidst COVID-19 Pandemic," 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2021, pp. 194-202, doi: 10.1109/CCICT53244.2021.00046.

[26] A. Gupta, R. Singh, V. K. Nassa, R. Bansal, P. Sharma and K. Koti, "Investigating Application and Challenges of Big Data Analytics with Clustering," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-6, doi: 10.1109/ICAECA52838.2021.9675483.

[27] Mamta, V. Veeraiah, D. N. Gupta, B. S. Kumar, A. Gupta and R. Anand, "Prediction of Health Risk Based on Multi-Level IOT Data Using Decision Trees," 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), Ghaziabad, India, 2023, pp. 652-656, doi: 10.1109/ICSEIET58677.2023.10303560.

[28] V. Veeraiah, N. B. Rajaboina, G. N. Rao, S. Ahamad, A. Gupta and C. S. Suri, "Securing Online Web Application for IoT Management," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1499-1504, doi: 10.1109/ICACITE53722.2022.9823733.

[29] K. A. Shukla, S. Ahamad, G. N. Rao, A. J. Al-Asadi, A. Gupta and M. Kumbhkar, "Artificial Intelligence Assisted IoT Data Intrusion Detection," 2021 4th International Conference on Computing and

Communications Technologies (ICCCT), Chennai, India, 2021, pp. 330-335, doi: 10.1109/ICCCT53315.2021.9711795.

[30] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Scalable Platform to Collect, Store, Visualize and Analyze Big Data in Real- Time," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118183.

[31] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "Detection of Liver Disease Using Machine Learning Approach," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1824-1829, doi: 10.1109/IC3I56241.2022.10073425.

[32] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Application of Deep Learning in Natural Language Processing," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1834-1840, doi: 10.1109/IC3I56241.2022.10073309.

[33] V. Veeraiah, V. Talukdar, S. B. Talukdar, J. Kotti, M. K. Dharani and A. Gupta, "IoT Framework in a Blockchain dependent Cloud Environment," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10308158.

[34] M. Dhingra, D. Dhabliya, M. K. Dubey, A. Gupta and D. H. Reddy, "A Review on Comparison of Machine Learning Algorithms for Text Classification," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1818-1823, doi: 10.1109/IC3I56241.2022.10072502.

[35] D. Mandal, K. A. Shukla, A. Ghosh, A. Gupta and D. Dhabliya, "Molecular Dynamics Simulation for Serial and Parallel Computation Using Leaf Frog Algorithm," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 552-557, doi: 10.1109/PDGC56933.2022.10053161

[36] K. A. Shukla, V. Juneja, S. Singh, U. Prajapati, A. Gupta and D. Dhabliya, "Role of Hybrid Optimization in Improving Performance of Sentiment Classification System," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 541-546, doi: 10.1109/PDGC56933.2022.10053333.

[37] V. V. Chellam, S. Praveenkumar, S. B. Talukdar, V. Talukdar, S. K. Jain and A. Gupta, "Development of a Blockchain-based Platform to Simplify the Sharing of Patient Data," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118194.

[38] Ashok, K., Chaturvedi, A., Agarkar, A. A., Ashraf, M., Ramesh, J. V. N., & Ambala, S. (2023). Fuzzy logic and cooperative hybrid least squares for improving network capacity and connectivity in high-density wireless networks. Optical and Quantum Electronics, 55(12), 1042.

[39] Uganya, G., Devi, C. S., Chaturvedi, A., Shankar, B. B., Ramesh, J. V. N., & Kiran, A. (2023). Sub-network modeling and integration for low-light enhancement of aerial images. Optical and Quantum Electronics, 55(11), 984.

[40] Godavarthi, B., Narisetty, N., Gudikandhula, K., Muthukumaran, R., Kapila, D., & Ramesh, J. V. N. (2023). Cloud computing enabled business model innovation. The Journal of High Technology Management Research, 34(2), 100469.

[41] Lakshmi, A. J., Kumar, A., Kumar, M. S., Patel, S. I., Naik, S. L., & Ramesh, J. V. N. (2023). Artificial intelligence in steering the digital transformation of collaborative technical education. The Journal of High Technology Management Research, 34(2), 100467.

[42] Sahoo, S. K., Nalinipriya, G., Srinivasan, P. S., Ramesh, J. V. N., Ramamoorthy, K., & Soleti, N. (2023). Development of a Virtual Reality Model Using Digital Twin for Real-Time Data Analysis. SN Computer Science, 4(5), 549.

[43] Balaram, A., Babu, R., Mahdal, M., Fathima, D., Panwar, N., Ramesh, J. V. N., & Elangovan, M. (2023). Enhanced Dual-Selection Krill Herd Strategy for Optimizing Network Lifetime and Stability in Wireless Sensor Networks. Sensors, 23(17), 7485.

[44] V. Talukdar, S. Bothe, R. Singh, R. Ponnusamy, U. Joshi and S. Talukdar, "Preventing Critical Information framework against Cyber-Attacks using Cloud Computing and Big Data Analytics," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1812-1817, doi: 10.1109/IC3I56241.2022.10072640.

[45] B. S. Rawat, D. Gangodkar, V. Talukdar, K. Saxena, C. Kaur and S. P. Singh, "The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 247-250, doi: 10.1109/IC3I56241.2022.10072877