International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

Advanced Analytics: Artificial Intelligence Applications in Preventing Fraudulent Transactions in Banking

Kriti Chourasiya
Research Scholar
Computer Science
R.N.T.U. Raisen
kritichourasiya86@gmail.com

Dr. S. Veenadhari
Professor, CSE
R.N.T.U.
Raisen
s.veenadhari@aisectuniversity.ac.in

Abstract*— Fraud prevention is a major consideration of most governments, corporations, and financial institutions in the world today. Complex fraudulent activities have been realized due to advancement in online business and complex financial markets. Artificial Intelligence (AI) provides creative answers to this expanding issue by using its capacity to evaluate enormous volumes of data, spot trends, and accurately forecast fraudulent activity. The use of AI for the identification of fraudulent banking operations is presented in this study. This study examines how ML and AI may be used to identify and stop fraud in the banking industry, a field that is becoming more and more susceptible to sophisticated cybercrime. As more people turn to electronic payments, financial corporations feel an increasing threat from scammers and fraudsters who might steal users' personal data or takeover their accounts. These are usual fraud risks that are not easy to combat through traditional methods of fraud detection and prevention. In this paper, techniques central to AI and ML, for example, supervised and unsupervised learning and reinforcement learning, major tasks like detecting anomalous activities, authenticity of customers, and risk evaluation are discussed. It further analyzes the prospects and impacts of AI-supported anti-fraud systems discuss challenges of AI and its possibilities for evolving the financial sector's perception of fraud and enhancing security and effectiveness in operations.

Keywords*— Fraud Prevention, banking sector, Fraud Detection, Data Privacy, Artificial Intelligence.

I. INTRODUCTION

The expansion of e-commerce, digital banking, and online transactions in the modern digital age has given fraudsters greater opportunities to exploit vulnerabilities in financial systems. Cybercrime is expanding, and more complex schemes are being used to attack governments, corporations, and people. These scams include anything from identity theft and phishing to more sophisticated financial frauds like money laundering and account takeovers. The rapid development of these fraudulent operations presents serious difficulties for conventional fraud detection and prevention techniques, which often fall behind the sophistication and agility of contemporary cybercriminals[1][2].

Technological developments and fraudulent activity are two dynamic aspects of the financial business that are always evolving. To protect their assets and preserve client trust in a constantly shifting environment, financial institutions must detect and prevent financial fraud. Conventional methods of detecting fraud, although sometimes effective, are often outmatched by the sophisticated strategies used by con artists. Figure 1 displays instances of banking fraud in India. However, developments in AI have radically altered methods for detecting and preventing financial fraud[3][4].

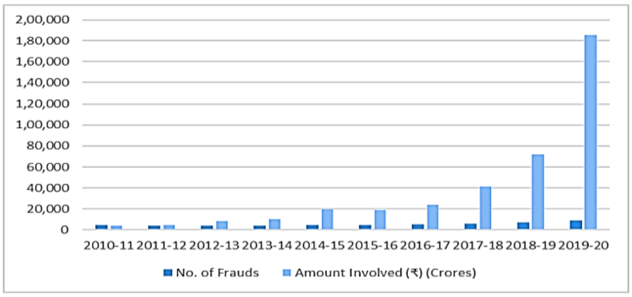

Fig. 1. Frauds Reported in Banks and Financial Institutions in India - Graphical Representation

A significant portion of large datasets from multiple sources including transactions, client data, and network activity logs are used to identify fraudulent financial activities using AI and ML. Hypers result in those algorithms shown as possible fraud signals various peculiarities: activity, transactions, or access beyond approval [5]. Artificial intelligence (AI) is changing the

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

way banks detect fraud. Financial institutions can detect and stop illicit financial activity before it causes significant harm due to ML algorithms [6]. Compared with methods of bank fraud detection of the past, which were mainly based on the reactive strategy, future analytical techniques, and machine learning make financial institutions employ proactive methods in fighting fraud efficiently[7][8].

1.1 Motivation of study

The steep growth of internet banking and other forms of digital transactions has prompted this investigation into the causes and consequences of financial fraud in the banking industry. Financial institutions risk huge losses and reputational harm because traditional fraud detection technologies can't keep up with the growing sophistication of criminals' tactics. With the global financial industry facing billions of dollars in fraud-related losses, there is a pressing need to adopt more advanced, efficient, and scalable solutions. An opportunity to radically improve fraud detection has arisen thanks to AI and ML, which can now provide real-time, predictive anomaly detection, allowing for the early identification of fraudulent behaviours. The goal of this research is to investigate how AI-driven models could enhance an accuracy, speed, and effectiveness of fraud detection, eventually giving banks a means to protect their resources and uphold customer confidence in a constantly changing threat environment.

1.2 Structure of paper

The following is the paper's structure: Section II provides a detailed description of Fraud in Banking and its types. AI for bank fraud detection in the banking sector are explained in section III. Section IV provides the background study of banking fraud prevention. Section V presents the paper's conclusion and plans for the future.

II. FRAUD IN BANKING SECTOR

Credit card providers treat fraud as a significant concern. In the USA, 800 million dollars were lost due to credit card fraud in 2004. The loss due to credit card theft in the same year is 425 million pounds, or around 750 million USD. Criminals orchestrated most of the fraud, and their primary tool is sophisticated fraud models. A major stumbling block to the development and efficiency of Chinese businesses is the tardiness of risk management. Researchers in the private financial business sectors of some Indian banks have made credit card risk management one of their most essential issues.

Frauds using credit cards result in billions of dollars in losses worldwide. Any activity taken to acquire financial advantage in any way without the cardholder's and the issuing bank's knowledge may be considered fraud. There are many methods to commit credit card fraud [9][10]. By stealing or misplacing cards, duplicating the original site, making counterfeit cards, skimming or stealing data from merchants, or by erasing or altering the magnetic strip on the card, which stores the user's information. In reality, fraud detection is a problem as it deals with the results of fraudulent activity amid thousands of real ones. Effective models must be created in order to prevent fraudulent schemes from being completed since fraudulent techniques are always evolving. Fraud in the financial sector may take many different forms. Among the frauds are:

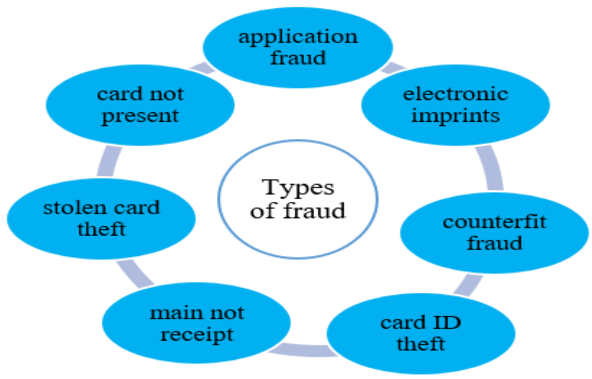

Fig. 2. Types of banking frauds

2.1 Application Frauds

The fraudster creates a fake account after gaining access to private user information, such as the login and password, and taking over the application system. It often occurs in relation to identity theft. When the fraudster uses the cardholder's identity to apply for credit or a new credit card [11].

2.2 Electronic Imprints

During the fraudster's skim of information put on the card's magnetic strip. The fraudster may utilise this information for future fraudulent transactions since it is highly sensitive and trustworthy [12].

2.3 Counterfeit Card Fraud

The most common method of attempting to commit counterfeit card fraud is skimming. A counterfeit or replica magnetic swipe card is created, including all of the original card's information. It is possible to promise future transactions using the well-designed replica fake card.

2.4 Card ID Theft

The fraud of card ID theft is similar to that of application fraud. In identity theft, the criminal obtains the original card's private information in order to use the card or create a new account. Fraud of this kind is very difficult to spot.

2.5 Stolen and Lost Card Fraud

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

In situations when the original cardholders lose their cards, fraudsters may get them and use them to make purchases. While using a machine to do this is challenging since a PIN is needed, the fraudster finds that internet transactions are rather simple.

2.6 CNP (Card Not Present)

A card may be used fraudulently even if the card's physical owner isn't known if the expiration date and account number are known.

2.7 Mail Non-Receipt Card Fraud

It takes time for the consumer to complete all the necessary processes when applying for a card. The criminal may use the card to make transactions if he registers it in his name if he intercepts the delivery in the midst of the process. Another name for this kind of scam is never received issue fraud.

Also, current systems can't tell the difference between legitimate and fraudulent transactions; they can only determine the likelihood of a transaction being fraudulent based on extensive customer spending data, behavioural analysis, and patterns of previously committed fraud.

III. AI For Bank Fraud Detection In Banking Sector

AI plays a transformative role in the banking sector by significantly enhancing fraud detection mechanisms through various advanced techniques. AI systems can identify unusual activity by analyzing account behavior and login patterns, flagging deviations that may signal fraudulent attempts. By tracking spending and deposit patterns, AI can recognize anomalies and notify bank personnel, while predictive models use historical data [13]to forecast future financial behavior, alerting the bank when abnormal patterns emerge. Data mining has the potential to uncover fraudulent activity in the banking industry. Data mining has raised the number of reported cases of fraud as many companies place a premium on detecting such instances. Artificial intelligence (AI) can be used in banking to detect fraudulent activity in a number of ways, including [14]:

- **Identifying unusual activity:** It can identify when an account is showing unexpected behavior or when a pattern of login has changed.
- **Tracking spending patterns:** In case of an issue, it informs workers and can track spending and deposit routines in the long term.
- **Building predictive models:** This way AI can know the tendency of the expenditures for the future and send notifications in case of any unusual activity.
- **Authenticating signatures:** AI can authenticate signatures and spot forgeries[15].
- **Analyzing text data:** The example in the email or chat structures AI can employ the natural language processing (NLP) [16] to look for the trademark of fraud.
- **Document verification:** AI can then validate such components as passports, signatures, account numbers, and others [17].
- **Risk scoring:** AI based risk scoring models use present day measures such as customer behavior and other repayments history and present-day transaction history.
- **Detecting image tampering:** New AI is capable of identifying high-level image manipulation and fakes [18].
- **Biometric authentication:** Modern banking solutions use facial recognition, fingerprints, and other traits as a way of approving large transactions [7].

AI leverages individual customer features to verify their identities and reduce the risk of unauthorized transactions.

IV. Machine Learning Overview

The phrase "machine learning" means "the automated detection of significant trends in data," which is a primary goal of this interdisciplinary area of study that straddles the intersection of computer science, mathematics, and statistics [19][20]. ML's many possible uses are almost endless and include, but are not limited to, the following: chess training, spam detection, image and speech recognition, prediction, and autonomous car power. The primary difference among humans and computers is that whereas computers need explicit instructions to learn, humans learn by their mistakes and other people's experiences. ML gives computers this ability, letting them "experience" (or learn from) their environment. ML, involves teaching a machine to do a task by observing human performance.

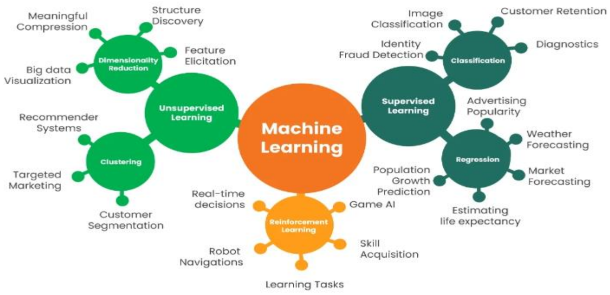

Fig. 3. Machine Learning Task Categories

Figure 3 provides a thorough breakdown of the 4 main types of ML tasks: semi-supervised learning, supervised learning, unsupervised learning, and reinforcement learning.

4.1 Supervised Learning

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

A dataset including inputs and outputs is used by supervised learning algorithms to build a mathematical model. A randomly selected portion of the whole dataset is often used as training data, also known as a collection of training examples. A supervisory signal is the intended result from training data, which takes one or more inputs. Each mathematical model's training datasets are represented by a feature vector, which may be either an array or a vector [21][22]. All of the training data is organised into matrices. In supervised learning, the algorithm takes its cues from a model that already has a function for predicting output given fresh inputs by optimising an objective function iteratively. A following workflow of supervised learning are as:

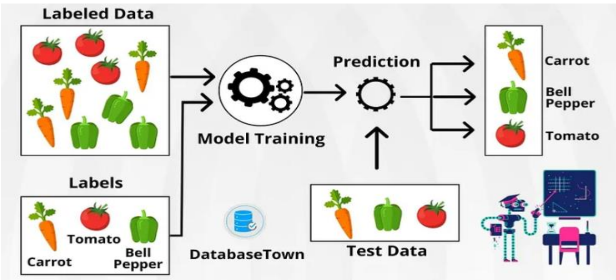

Fig. 4. Supervised learning workflow

4.2 Unsupervised machine learning

Unsupervised ML techniques are perfect for description work since their objective is to identify correlations in a data structure without generating a measurable result. Unsupervised ML describes this kind of ML as it does not rely on a response variable to direct the research [23][24]. Unsupervised learning focusses on identifying patterns and relationships in a dataset that were previously unknown. Although supervised learning will be our primary focus later on, unsupervised learning encompasses methods such as PCA, factor analysis (FA), and mixture modelling, all of which are often used in psychological categorisation and psychometric research. Figure 5 illustrates the unsupervised learning procedure.

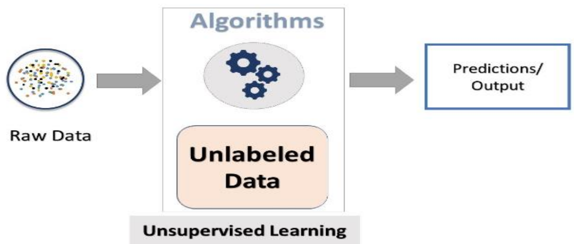

Fig. 5. Unsupervised learning

4.3 Reinforcement learning

Reinforcement learning is a ML technique that allows computers and software programs to automatically choose the best way to behave in a certain situation. An environment-driven approach might be one way to describe the method used in this kind of learning. The ultimate objective of this kind of education is to use the information that environmental activists have imparted to make changes that will either lessen the danger or enhance the benefit. It is not recommended for solving the most fundamental problems, even if it performs well for training AI models[25]. Supply chain logistics, robotics, self-driving automobiles, and assembly are a few examples of these procedures [26]

Fig. 6. Reinforcement Learning

The following methods are used to prevent banking fraud operation recognition.

V. LITERATURE REVIEW

An increasing number of academics have been devoting time and energy to studying ways to use AI to identify fraudulent banking operations in recent years. Some background studies are provided below:

In this research Balaji et al., (2024) a complete approach is introduced that makes it easier to spot fraud in banking systems. The system has algorithms for machine learning, important management parts, and big data analytics. using "big data" technologies to collect and examine a lot of data from a lot of different sources, such as external data streams, internal transaction records, and profiles of customers. Fraud detection systems get better at telling the difference by picking out key features from preprocessed data. Researching on a system that will constantly watch all incoming transfers and send alerts right away if any suspicious activity is seen. For this reason, it becomes essential to control, establish the warning mechanism, and find the ways of identifying scrupulous signs. This is why the financial industry needs to make sure that the techniques used in identifying and mitigating the fraud are legal and relevant to its compliance obligations [27] .

This research Sheth et al., (2024) is concerned with the development and assessment of complex anti-fraud programs to properly address this critical issue. In addition to traditional ML

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

methods, the research makes use of advance DL models including LSTM, FNN, and Recurrent Neural Network (RNN) to accomplish this. These models are trained with big data sets to identify hints of fraudulent transactions that can be employed to high-light the cases. These DL architectures greatly improve the efficacy and precision of fraud detection procedures due to the complex interaction between transactional data, customer behaviour, and temporal correlations [28].

In this paper Thar and Wai, (2024) the main objective of this challenge is to provide a novel intelligent ensemble approach to fraud transaction detection that is both autonomous and successful. Probabilistic models for sequences of observations allow Hidden Markov Models (HMM) to reveal the hidden states of financial transactions, which are predicated on the belief that the underlying process is a Markov process with hidden states. And then, machine learning model called Gradient Boosting Classifier (GBC) is applied to classify the fraud. Furthermore, our combined approach combines GBC and HMM. If HMM and GBC are to be effective, experiments must be performed [29].

In Backiyalakshmi and Umadevi, (2023) the details of the prior fraud detection techniques employing ML and DL are discussed. Here, the brief introduction to fraud detection in the banking sector, the existing literature works regarding fraud detection, and the chronological assessment of fraud detection are presented in an elaborate way. In this review, the existing techniques used for banking security are discussed. Moreover, the simulation tools and the performance indices adopted for fraud detection in the banking sector are discussed. Lastly, the research gaps and challenges the given for future research studies [30].

This study Dash et al., (2023) compares and contrasts traditional methods of ML, such as DT and LR, with more recent methods, such as neural networks. The results show that neural networks outperform more traditional methods when tested with real-world financial and banking data. Furthermore, our study highlights how data collection and management play a crucial role in the development of fraud detection systems [31] .

This paper Sankar Roy, Ebtidaul Karim and Biswas Udas, (2022) provide an algorithm for detecting blockchain fraud using deep learning, fed by data from the Ethereum blockchain. To identify fraudulent actions in the system, we construct a detection model based on deep learning and link it to a trustworthy dataset in the relevant domain. The suggested classification model for identifying fraudulent transactions uses a dense unit in conjunction with a LSTM unit. Information Gain has been used as the model's feature selection unit in order to simplify things and eliminate superfluous transactional features. Experimental findings demonstrate considerable improvements in several areas when using the suggested technique, as compared to the comparable values of alternative models on the same dataset [32].

In this paper Janet, Joshua Arul Kumar and Ganesh, (2022) examine the methods used by conventional ML algorithms in dealing with data that is skewed towards fraudulent transactions and contrast them with algorithms developed for handling such data. An evaluation and comparison of several supervised ML models (LR, DT, RF, and SVM) is conducted with the aim of detecting fraud in mobile money transactions. A synthetic dataset, created using a simulator based on actual corporate transactions, is used to evaluate all classification algorithms [33].

Table 1 review the summary of background study includes the findings, features and , the limitations of each study.

TABLE I. SUMMARY OF RECENT STUDIES ON ARTIFICIAL INTELLIGENCE FOR FRAUDULENT BANKING OPERATIONS RECOGNITION

Author	**Techniques**	**Key Features**	**Findings**	**Limitations**
Balaji et al.	Machine Learning, Big Data Analytics	External data streams, Internal transaction records, Customer profiles	Introduced a complete approach to fraud detection using feature extraction from big data.	Does not specify model performance metrics or focus on specific machine learning algorithms.
Sheth et al.	LSTM, FNN, RNN	Temporal relationships, Consumer behavior	Deep learning models outperform traditional methods in detecting fraud based on transactional data.	Computationally expensive due to deep learning models, may face challenges in real-time detection.
Thar and Wai	Hidden Markov Model (HMM), Gradient Boosting Classifier (GBC)	Probabilistic models, Markov process with hidden states	Hybrid method combining HMM and GBC shows effectiveness in fraud detection.	Limited to financial transaction sequences, may not generalize well to other domains.
Backiyalakshmi and Umadevi	Review of ML and DL techniques	Chronological assessment of fraud detection	Provides an overview of fraud detection techniques and highlights research gaps for future work.	Does not propose a specific model or solution, only reviews existing techniques.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 9, September 2024)

Dash et al.	Neural Networks, Logistic Regression, Decision Trees	Data gathering and management, Real-world financial data	Neural networks outperform traditional models in detecting fraud. Emphasizes importance of data management.	Limited comparison with other advanced deep learning models like LSTM or RNN.
Sankar Roy, Ebtidaul Karim, and Biswas Udas	DL, Blockchain, LSTM	Information Gain for feature selection, Ethereum blockchain data	Blockchain-based deep learning model shows improved fraud detection accuracy.	Complexity of blockchain and deep learning integration, scalability concerns for large datasets.
Janet, Joshua Arul Kumar, and Ganesh	Logistic Regression, Random Forest, Decision Tree, SVM	Imbalanced data handling, Synthetic datasets	Comparison of traditional ML models in handling imbalanced data for mobile money transaction fraud.	Focuses on synthetic datasets; real-world applicability is unclear.

VI. CONCLUSION AND FUTURE WORK

Technological growth brings various fields into linear advancement, the banking domain is one among these and it deals with financial activities. There are some key enabling strategies like big data, cloud computing, AI, ML, and the IoT are utilized to enhance security in the banking domain. AI and ML have revolutionized fraud detection in the banking sector by offering advanced, data-driven techniques that enhance the accuracy, speed, and efficiency of identifying and preventing fraudulent activities. AI enables banks to adopt a proactive approach, identifying suspicious behaviors in real-time and automating the analysis of vast amounts of transaction data. Furthermore, AI techniques such as biometric authentication, document verification, and risk scoring enhance security while streamlining banking operations. While AI-powered solutions have made significant strides in fraud detection, there remain challenges related to the complexity of fraud schemes, data privacy concerns, and the need for continued technological advancements. Future work should focus on enhancing AI models' ability to handle more complex and evolving fraud schemes by incorporating more diverse data sources, including social media, dark web data, and behavioral analytics.

REFERENCES

[1] Oluwabusayo Adijat Bello and Komolafe Olufemi, "Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities," *Comput. Sci. IT Res. J.*, vol. 5, no. 6, pp. 1505–1520, 2024, doi: 10.51594/csitrj.v5i6.1252.

[2] H. Sinha, "The Identification of Network Intrusions with Generative Artificial Intelligence Approach for Cybersecurity," *J. Web Appl. Cyber Secur.*, vol. 2, no. 2, pp. 20–29, Oct. 2024, doi: 10.48001/jowacs.2024.2220-29.

[3] Ms. Vibhuti Talreja, V. Sanjay Kumar, Vignesh S, and Sujith Pandi.T, "a Survey of Ai on Financial Fraud Detection," *EPRA Int. J. Environ. Econ. Commer. Educ. Manag.*, no. 5, pp. 154–157, 2024, doi: 10.36713/epra16794.

[4] P. K. and S. Arora, "THE IMPACT OF MACHINE LEARNING AND AI ON ENHANCING RISK-BASED IDENTITY VERIFICATION PROCESSES," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 06, no. 05, pp. 8246–8255, 2024.

[5] J. Jansen and R. Leukfeldt, "How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases," in *Proceedings - 5th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2015*, 2015. doi: 10.1109/STAST.2015.12.

[6] S. Ahmed, R. K. Chakrabortty, and D. L. Essam, "Predictive big data analytics for supply chain demand forecasting," in *Computational Intelligence Techniques for Sustainable Supply Chain Management*, no. June 2022, Elsevier, 2022, pp. 301–330. doi: 10.1016/B978-0-443-18464-2.00011-X.

[7] P. Khare and S. Srivastava, "AI-Powered Fraud Prevention: A Comprehensive Analysis of Machine Learning Applications in Online Transactions," *J. Emerg. Technol. Innov. Res.*, vol. 10, pp. f518–f525, 2023.

[8] R. Goyal, "EXPLORING THE PERFORMANCE OF MACHINE LEARNING MODELS FOR CLASSIFICATION AND IDENTIFICATION OF FRAUDULENT INSURANCE CLAIMS," *Int. J. Core Eng. Manag.*, vol. 7, no. 10, pp. 34–44, 2024.

[9] L. Delamaire, H. Abdou, and J. Pointon, "Credit card fraud and detection techniques: A review," *Banks and Bank Systems*. 2009.

[10] H. Sinha, "An examination of machine learning-based credit card fraud detection systems," *Int. J. Sci. Res. Arch.*, vol. 12, no. 01, pp. 2282–2294, 2024, doi: https://doi.org/10.30574/ijsra.2024.12.2.1456.

[11] H. Ahmad, B. Kasasbeh, B. Aldabaybah, and E. Rawashdeh, "Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS)," *Int. J. Inf. Technol.*, 2023, doi: 10.1007/s41870-022-00987-w.

[12] M. A. Kabir, S. Z. Saidin, and A. Ahmi, "Adoption of e-Payment Systems: A Review of Literature," in *Proceedings of the International Conference on E-Commerce (ICoEC) 2015*, 2015.

[13] H. Sinha, "Predicting Bitcoin Prices Using Machine Learning Techniques With Historical Data," *Int. J. Creat. Res. Thoughts*, vol. 12, no. 8, 2024, doi: 10.3390/e25050777.

[14] K. Mullangi, N. D. Vamsi Krishna Yarlagadda, and M. Rodriguez, "Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 5, no. 1, pp. 42–52, 2018.

[15] P. Khare and I. Researcher, "SIGNATURE-BASED BIOMETRIC AUTHENTICATION: A DEEP DIVE INTO DEEP LEARNING APPROACHES," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 4, no. 8, Aug. 2022, doi: 10.56726/IRJMETS29522.

[16] H. Sinha, "ANALYZING MOVIE REVIEW SENTIMENTS ADVANCED MACHINE LEARNING AND NATURAL LANGUAGE PROCESSING METHODS," *Int. Res. J. Mod. Eng. Technol. Sci.* (, vol. 06, no. 08, pp. 1326–1337, 2024.

[17] P. Khare, "Transforming KYC with AI : A Comprehensive Review of Artificial Intelligence-Based Identity Verification," vol. 10, no. 12, pp. 525–531, 2023.

[18] H. Sinha, "Advanced Deep Learning Techniques for Image Classification of Plant Leaf Disease," *J. Emerg. Technol. Innov. Res.*

www.jetir.org, vol. 11, no. 9, pp. b107–b113, 2024.

[19] S. Shalev-Shwartz and S. Ben-David, *Understanding machine learning: From theory to algorithms*. 2013. doi: 10.1017/CBO9781107298019.

[20] R. Tandon, "The Machine Learning Based Regression Models Analysis For House Price Prediction," *Int. J. Res. Anal. Rev.*, vol. 11, no. 3, pp. 296–305, 2024.

[21] S. Aggarwal and Anmol, "Health Insurance Amount Prediction Using Supervised Learning," in *Proceedings of International Conference on Technological Advancements in Computational Sciences, ICTACS 2022*, 2022. doi: 10.1109/ICTACS56270.2022.9988256.

[22] K. Mullangi *et al.*, "AI-Augmented Decision-Making in Management Using Quantum Networks," *Asian Bus. Rev.*, vol. 13, no. 2, pp. 73–86, Aug. 2023, doi: 10.18034/abr.v13i2.718.

[23] R. James, G., Witten, D., Hastie, T., Tibshirani, *An Introduction to Statistical Learning - with Applications in R | Gareth James | Springer*. 2013.

[24] S. C. R. V. Bhavik Patel, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, Kishore Mullangi, "Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering," *Eng. Int.*, vol. 10, no. 2, pp. 117–130, 2022.

[25] J. Thomas, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.

[26] T. M. Moerland, J. Broekens, A. Plaat, and C. M. Jonker, "Model-based Reinforcement Learning: A Survey," *Foundations and Trends in Machine Learning*. 2023. doi: 10.1561/2200000086.

[27] K. Balaji, N. Saxena, N. R. Behera, M. Kiran Kumar, H. K. Prasad, and P. R. Gedamkar, "Improved Fraud Detection in Banking Systems through Machine Learning and Big Data Analytics with Management Key Components," in *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 2024, pp. 1–6. doi: 10.1109/ACCAI61061.2024.10601803.

[28] A. Sheth, A. Nair, A. Rai, and R. Sawant, "Prediction and Analysis of Fraud Detection in Finance: A Deep Learning and Machine Learning based approach," in *2024 4th International Conference on Intelligent Technologies (CONIT)*, 2024, pp. 1–6. doi: 10.1109/CONIT61985.2024.10626214.

[29] K. W. Thar and T. T. Wai, "Machine Learning Based Predictive Modelling for Fraud Detection in Digital Banking," in *2024 IEEE Conference on Computer Applications (ICCA)*, 2024, pp. 1–5. doi: 10.1109/ICCA62361.2024.10532788.

[30] V. Backiyalakshmi and B. Umadevi, "A Systematic Short Review on Intelligent Fraud Detection Approaches in the Banking Sector using Deep Learning and Machine Learning with Future Trends," in *2023 6th International Conference on Recent Trends in Advance Computing (ICRTAC)*, 2023, pp. 474–481. doi: 10.1109/ICRTAC59277.2023.10480811.

[31] S. Dash, S. Das, S. Sivasubramanian, N. Kalyana Sundaram, G. K. Harsha, and T. Sathish, "Developing AI-based Fraud Detection Systems for Banking and Finance," in *Proceedings of the 5th International Conference on Inventive Research in Computing Applications, ICIRCA 2023*, 2023. doi: 10.1109/ICIRCA57980.2023.10220838.

[32] K. Sankar Roy, M. Ebtidaul Karim, and P. Biswas Udas, "Exploiting Deep Learning Based Classification Model for Detecting Fraudulent Schemes over Ethereum Blockchain," in *2022 4th International Conference on Sustainable Technologies for Industry 4.0, STI 2022*, 2022. doi: 10.1109/STI56238.2022.10103259.

[33] B. Janet, R. Joshua Arul Kumar, and D. P. S. Ganesh, "Credit Card Fraud Detection with Unbalanced Real and Synthetic dataset using Machine Learning models," in *Proceedings of the 2022 International Conference on Electronic Systems and Intelligent Computing, ICESIC 2022*, 2022. doi: 10.1109/ICESIC53714.2022.9783529.