IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025

DOI: 10.17148/IJARCCE.2025.14718

AI Based Fraud Detection in Cybersecurity: Applications in Financial Services

Dinesh Kumar Budagam

Visa Inc, Foster City, USA

Abstract: In the current digital era, financial cybersecurity is crucial, where the financial industry is vital to the world economy. The frequency and sophistication of cyber-attacks are mounting, making difficult for traditional fraud detection systems to stay up with the changing threats. As a consequence, using Artificial Intelligence (AI) based Machine Learning (ML) approach in fraud detection system, the presented article offers an enhancing financial cybersecurity. The collected input data from financial and transactional data gets pre-processed with the help of data cleaning, data normalization, which aims to remove noise and improve the quality of input data. For effectual forecasting of fraud prediction, the proposed model uses a novel hybrid rule based and isolation forest approach. This rule based scheme ensures regulatory compliance and interpretable alerts, while the isolation forest proficiently isolates anomalies without requiring labeled data. Overall, the analytical evaluation on real world financial transactions system is ensured by the introduced topology, which accomplishes lower errors and higher accuracy of (97.45%) with a significant reduction in false positives and faster decision making compared to the traditional supervised learning models.

Keywords: Financial cybersecurity, cyber-attacks, fraud detection systems, Artificial Intelligence, Machine Learning, Hybrid rule based and isolation forest.

I. INTRODUCTION

An extraordinary enhancement in financial fraud attempts have provoked by the digital transformation of banking services, making traditional security measured progressively less effective [1]. According to recent worldwide data, financial services handle about 1.7million transaction a year and losses from fraudulent activity amount over $42 billion [2]. One of the most crucial strategies for preventing financial fraud while preserving operational effectiveness is the use of AI and data science topologies [3]. The banking industry has a number of complex problems with fraud detection such as need for real time analysis, handling unbalanced datasets and adjusting to changing fraud trends. The classical rule based system provide fundamental security safeguards, but owing to its static nature, they are becoming less effective against complex fraud schemes that take use of new weakness and developing technology [4-5]. According to available data, detection system only detect 70% of fraudulent transactions and generate a significant number of false positives that need to manually reviewed. As banking uses more advanced technologies, strong cybersecurity measures like AI driven threat detection are essential [6].

A. Banking Fraud and Cybersecurity: An Overview and Development

A wide range of illegal behaviours that have changed dramatically with technological advancements are included in financial fraud in banking [7]. According to recent studies, researchers are using automation and AI more to plan complex assaults, which leads to a dynamic threat landscape that requires equally sophisticated detection and prevention systems [8]. One particularly difficult development in financial crime is synthetic identity fraud. Authors develop synthetic identities that circumvent conventional verification methods by incorporating authentic and fake information according to the analysis. Synthetic identity fraud is responsible for 18% of all fraud losses in the banking industry and 23% of credit card losses according to the thorough analysis of 200,000 fraud instances [9-10].

Rule based systems and manual review procedures are the mainstays of earlier banking security strategies [11]. Based on the investigation of 150 financial institutions, classical rule based system often produce false positive rates over 30% and detect less fraudulent transactions. These outcomes indicates that how static rule sets are unable to keep up with changing fraud trends [12].

B. Modern AI based ML scheme for predicting banking fraud

ML algorithm is one of the AI scheme used by contemporary fraud detection systems. This model is deployed owing to its proven efficacy in actual banking settings and its exceptional flexibility in dealing with new forms of fraud [13]. This topology handle large volumes of transactions in real time while preserving accuracy and scalability over a banking processes are prioritised in the selection criterion [14].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025

DOI: 10.17148/IJARCCE.2025.14718

AI-driven system accomplish average detection rates of 91% while keeping safe positive rates below 10%, according to recent meta-analysis of 85 implementations over major financial institutions. In applications for fraud detection, supervised learning models have proven especially effective [15-16]. Random forest model identify 92% accuracy, according to a comparative study of different algorithms on comparable datasets. Strong evidence for the performance of ensemble approaches in managing unbalanced datasets typical fraud detection found in studies that include 10 million transactions from 15 banks [17]. K-Nearest Neighbour (KNN) [18] maps transaction features to higher dimensional space, which is an outstanding at spotting minute behavioural distinctions over fraudulent and lawful activity. KNN's attained good detection accuracy with tolerable model inference times according to the implementation analysis. With high detection rates for this rising common attack vector, KNN's signifies a special ability to detect account takeover fraud.

The gradient boosting approaches such as XGboost and LightGBM have shown remarkable performance [19-20]. Analysis of transactions handled by gradient boosting models showed that effective processing speeds are maintained while high detection accuracy is maintained. These models perform exceptionally well in identifying fraudulent activity in high value transactions. Without requiring total retraining, their capacity for incremental learning allows for ongoing enhancement.

TABLE I FRAUD DETECTION USING MACHINE LEARNING [21]

Approaches	Type and applications	Key findings	Limitations
SVM	Supervised- application fraud	Good performance for binary classification tasks common in fraud detection.	Computationally intensive with large datasets
Neural Networks	Supervised-multi channel detection	Automatically extract features with minimal manual preprocessing.	Prone to overfitting if not properly regularized.
Isolation forests	Unsupervised- real time anomalies	Fast and suitable for real time detection scenarios	Less precise for fraud patterns compare to the supervised models.
Random forest	Supervised- card transactions	Handles large datasets and high dimensionality well	Less effective if fraud patterns change rapidly over time.
Graph analysis	Hybrid-fraud networks	It captures complex relationships and interactions over entities (users, transaction)	Requires high quality, well-structured data to complexity.

The above mentioned issues has to be rectified by presenting a novel topology, thereby the proposed work utilizes hybrid rule based and isolation forest approach and overall contributions are discussed below,

- ✓ AI based ML plays an essential role in improvising financial cybersecurity by accurately detecting fraudulent activities over real time analysis.
- ✓ Data cleaning and normalization based preprocessing model deployed for eliminating noise and enhance the quality of input data.
- ✓ Integrating hybrid rule based and isolation forest approach to enhance the prediction accuracy with better detection rate, thereby identifying threats and adaptability to new, unknown fraudulent activities.

II. SYSTEM MODEL

A. Banking and Financial Services

AI-driven fraud detection is crucial in banking industry to fight against threat, account takeover attacks and credit card fraud. To examine transaction patterns and spot irregularities, ML based models such as RF, Logistic Regression and more recently employed, which has the ability to identify suspicious activity based on geolocation or temporal irregularities. These model's main benefits is its extraordinary speed and accuracy in identifying known fraudulent patterns. Its incapacity to determine zeroday frauds, novel forms of fraud, unless regularly retrained, which is a significant drawbacks faced by this models, leads to produce false positives that interfere with valid transactions [22].

B. E-commerce and Online Retail

In e-commerce, fraud detection focuses a fake accounts, payment fraud and return fraud. Here, SVM, Gradient Boosting Machines (GBMs) are commonly deployed owing to its capacity to handle imbalanced datasets and high dimensional feature spaces.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025
DOI: 10.17148/IJARCCE.2025.14718

The advantage of deploying these models lies in its classification abilities, especially in distinguishing over fraudulent and genuine user behaviours in real time. However, they often suffer from poor interpretability, making it difficult to explain decisions to non-technical stakeholders. Moreover, these schemes requires continuous feature engineering and updating to stay ahead of evolving fraud topologies [23].

C. Insurance Sector

In insurance fraud detection (i.e auto claims, health insurance) unsupervised topologies such as autoencoders, K-means clustering are applied to identify irregular claims patterns without labeled data. These models are mainly benefits owing to uncover prior unknown fraud patterns, minimizing dependence on historical labeled datasets. Nevertheless, they face limitations like sometimes be flagged as suspicious, hereby enhancing investigation overhead and customer dissatisfaction [24].

D. Telecommunication

Telecom fraud, such as SIM cloning, subscription fraud and call spoofing is adequately using Bayesian networks, hidden markov models and Decision tree models, model sequences of call records. The strength of these lies in its ability to capture temporal dependencies and produce predictive insights. Nonetheless, their significant drawbacks is the essential for large volumes of time series data and computational resources for real time processing, mainly in large scale telecom applications [25].

E. Healthcare and Medical Systems

In healthcare, AI is deployed for finding billing fraud, up coding and phantom billing over models such as Decision tree (DT), Naïve Bayes and ensemble classifiers. This approaches provide rapid, interpretable decision making that is useful in regulated domains like healthcare. A significant advantages is the model's transparency, indicates in understanding why a particular claim is flagged. Although, its main limitations is provider's data not perform well over various hospital systems owing to variations in coding practices [26].

F. Government and Tax Systems

Government agencies utilize AI models to detect benefit fraud, tax evasion and procurement scams. Hybrid models that combine supervises and unsupervised learning including XGboost is utilized. This models finding accurately both known and unknown fraud with the aid of holistic detection strategy. Moreover, incorporating various models enhances system complexity and maintenance costs and results in conflicting outcomes requiring manual adjudication [27].

Overcoming the Drawbacks of Conventional Approaches

In financial cybersecurity, conventional fraud detection system adequately suffer from high false positive rates, a lack of flexibility in responding to new fraud trends and subpar data that minimizes detection accuracy. These systems generally rule based, static procedures or need a lot of labelled data, which aren't requires practical in real time settings. By incorporating intelligent pattern recognition and real time analytical processing, the presentenced AI based ML models highly improves fraud detection skills to overcome these constraints. The model ensures dynamic adaptation to changing fraud strategies, which classical systems adequately skip, by permitting continual learning from real time transaction data. The proposed model provides a scalable standard for financial in fraud detection in cybersecurity applications.

III. PROPOSED SYSTEM

A structured framework for fraud detection system using hybrid rule based and isolation forest approach as represented in Fig. 1. The data sources serve as a main sources of raw financial and transactional data, which fed to data collection process, where the data is aggregated for additional analysis. Subsequently, the data gets pre-processed via data cleaning and normalization, which is the essential step for ensuring the input is accurate by eliminating noises. Moreover, the cleaned data is then fed to fraud detection module, that uses a hybrid rule based and isolation forest model for effective classification of fraud prediction. The system has the ability to precisely spot fraudulent patterns in the data via the hybrid model.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025

DOI: 10.17148/IJARCCE.2025.14718

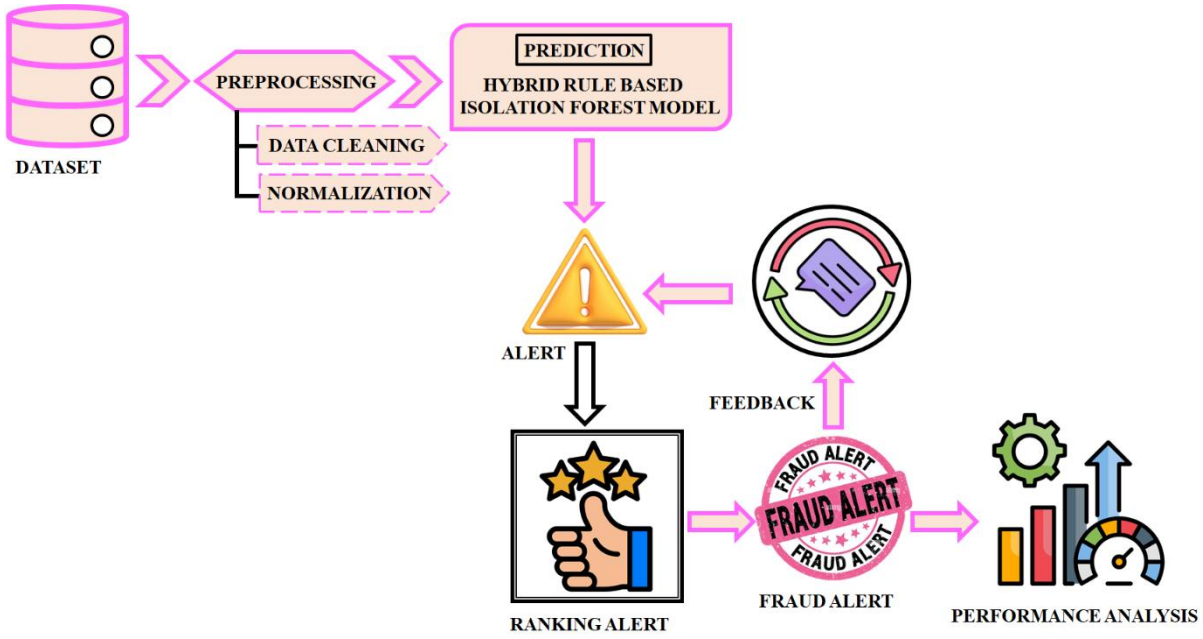

Fig. 1 Representation of fraud prediction using ML

Consequently, the alert and reporting module receives the findings of the fraud detection process, which completes the detection and reaction loop in financial security system by producing alerts for questionable activity and producing thorough reports for the analysis or decision makers.

A. Data Collection

In AI based fraud detection system for financial cybersecurity, data gathering is a fundamental step owing to the quality, diversity and volume of data used to train the detection model highly. Usually, data in this context is compiled from a variety of sources inside the financial ecosystems, such as transactional databases, network level metadata, user behavioural logs, customer profiles and device fingerprinting. Features including transaction ID, date, amount, merchant category, location and payment method are all included in transaction data. A typical usage patterns is detected by analysing behavioural data, contains user login frequency, session length, typing habits and access devices. It is also possible to incorporate information from third party threat intelligence feeds, blacklist databases and fraud monitoring systems to enhance detection granularity and extend the feature space. A novel model is required in real world financial system since the data adequately shows class imbalance with legimate transactions highly predicting fraudulent ones.

B. Preprocessing Model

Data Cleaning

Data cleaning is an essential preprocessing step in financial fraud prediction system, aims to ensure the input data is accurate, consistent ad of high quality before sent into prediction model. Missing values, duplicate records, mismatched formats are leads to the formation of noise in transaction data. These come from a variety of causes, including logging mistakes, system latencies. Moreover, to avoid data leakage and model bias, duplicate records, which results from repeated API calls are determine and eliminated using record hashing. During this phase, outlier detection is also used to find and mark records that show odd trends high transaction volumes.

Data Normalization

After the data cleaning phase, normalization is applied to make sure that the features in the data are on a similar scale, which is crucial for preserving numerical stability and enhancing model performance in fraud prediction in financial sector. Features having various stages such as transaction amounts, account balances and frequency counts are adequately found in input data. Models gets biased towards features with higher magnitude if normalization is not applied. One of the normalization model is min-max scaling, used to bring all features into a consistent range. Additionally, logarithmic transformation is deployed to minimize variance and improve model convergence for highly skewed data like purchase amounts. These topology boost up the convergence rates, guarantee balanced input for ML models.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025

DOI: 10.17148/IJARCCE.2025.14718

C. Hybrid Rule Based and Isolation Forest Approach

To build a cybersecurity detection model, the first phase is to define the training data, made up of labelled recorded that indicates numerous financial activities. Device ID, IP address, geolocation, frequency, transaction time, type, amount, source account behaviour and other metadata are all included in each record. For cybersecurity, these attributes are not directly sent to the rule generation model. Instead, they are transformed into a decision supporting format. This involves determining threshold based conditions for each attribute. For example:

- ✓ A characteristics like transaction frequency is assessed for weather it exceeds a behavioural norm.
- ✓ Geolocation mismatch over user location and transaction origin is tested for deviation.

Each features undergoes a binary conversion depend on the above mentioned condition, if the condition holds (i.e frequency >historical median) a binary value 1 is given, or else it is 0. This conversion process transform the data into a format suitable for rule induction each transaction is now a structures combination of binary decisions.

Transaction Clustering

To predict behavioural patterns, transactions are grouped using a clustering process based on binary vector indicating attribute conditions. This phases serves two purposes such as,

- ✓ It uncovers latent danger categories and user behavioural groupings.
- ✓ It split transactions with comparable attack or operational patterns (i.e- cross border anomalies, quick fund transfers.

A centroid based clustering algorithm is deployed, each cluster represents a prototypical transaction pattern. The model iteratively assigns transactions to clusters by reducing the hamming distance over a transaction and cluster centroids. After convergence, the cluster are labeled based on security analysts. This permit the downstream rule engine to treat each cluster as a distinct threat or behavioural class.

Sequence Pattern Mining

This stage extracts frequently occurring patterns over transaction sequences within every cluster. These sequences represent temporal or contextual changes in transaction behaviour as,

- ✓ Device switching over geographical areas.
- ✓ Smurfing is the practice of repeatedly making small transfers before making a big one.
- ✓ Brief bursts of login, transaction and logout sequences.

The mining algorithm identifies ranges of attributes values over transactions in the same cluster. These ranges are generalized into bounds, lower and upper thresholds for each attribute, making value interval conditions. For instance, if various transactions in a cluster show login times within a specific off peak window and transaction amounts within a certain range. These values bounds are stored, these form the building blocks of the rule terms, respectively.

Rule Construction

The mined attribute value intervals and transaction class are utilized to build each rule in the system. The traditional IF-THEN format is deployed to structure rules.

IF: a conjunction of conditions on attribute intervals (login time over X and Y transaction amount within range A to B, location mismatch= true).

THEN, a classification of the transaction (Flag as anomalous, Trigger as risk score elevation and route for analyst review).

The construction process begins with frequent pattern item sets and grows the rules iteratively by combining these intervals using logical AND operators. Every combination is tested for consistency and coverage on the training dataset. Rules are only retained if they satisfy initial convergence thresholds (i.e they match a sufficient number of transactions) and do not conflict with known normal behaviours.

Confidence and Support Evaluation

To measure rule quality, two crucial metrics are utilized as,

- ✓ **Support:** it measures how frequently a rule's condition arise in the data, a high level of support indicates that a common pattern is captured by the rule.
- ✓ **Confidence:** Shows the likelihood that the outcome such as that the transaction is indeed unusual, which accurately predicted when the requirements of the rule are satisfied.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025

DOI: 10.17148/IJARCCE.2025.14718

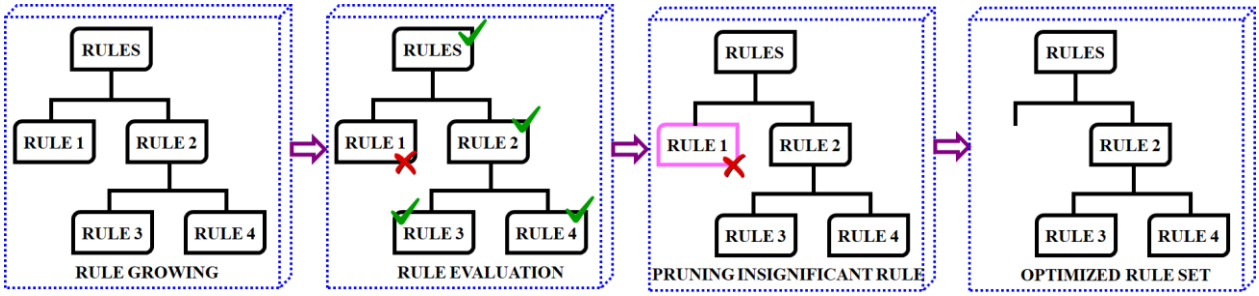

Fig. 2 Process of rule optimization

Rule Set Refinement

This model focuses on enhancing the proficiency of rule set, redundant rules and low performing rules are discarded. Moreover, the system searches for rule generalizations, merging similar rules by relaxing around attribute intervals or extracting unnecessary conditions, which ensure

- ✓ **Generalizability-**Rules detect new, unseen variations of threats
- ✓ **Efficiency-** Slight rules leads to speedy real time evaluation

The final outcomes is a clean and non-redundant rule base that maintains high detection performance.

Structural and Consistency Verification

Prior utilizing the rule set into a cybersecurity engine, each rule is verified for structural integrity,

- ✓ **Syntax check-** the rules confirm to logical structure (i.e no missing condition operators, no overlapping intervals).
- ✓ **Consistency check-** ensuring that no two rules generate contradictory decisions for similar transaction pattern. A rule conflict resolution mechanism is deployed, where more confidence rules take precedence.

The verification step ensures that the rule set is robust, interpretable and free from functional uncertainties.

Real time Cybersecurity Detection

The rule set is compiled into an executable rule engine by deploying a condition evaluation structure, typically integrated through a ML classifier.

- ✓ If a transaction matches any rule's condition, it is flagged.
- ✓ The model assign a severity level or forward the transaction to a manual review module.
- ✓ Additionally, risk scores are updated dynamically based on rule hits.

This allows the cybersecurity scheme to function in real time, generating prompt alerts for doubtful behaviours while reducing false positives over high confidence rules.

Isolation Forest Model

The isolation forest algorithm is a decision tree based model mainly used to anomaly prediction, appropriate for determining fraudulent patterns from various data collected. The main aim of this model is that fraudulent transactions are fundamentally easier to isolate from the rest of the data than legimate ones. The algorithm works by randomly selecting features and splitting values to recursively partition the collected data. This partitioning procedure continues until all data points are isolated. Owing to its similarity and concentration in the data space, requires higher partitioning phased to be splitted, whereas fraud instances deviate significantly and therefore needed some partitions for isolation. The repeated partitioning of data points is signified using a tree structure known as an isolation tree. Within this structure, anomalies appear with shorter path lengths because they are easier to isolate, whereas normal points results in longer paths owing to the higher number of splits required. An isolation tree is constructed by recursively splitting the data until all instances are isolated or a predefined maximized tree depth is attained.

During the detection process, anomaly scoring is carried by evaluating the average path lengths over all isolation tress for a give data. This score is indicative of how easily the point is divided from the rest of the data. Shorter average path lengths correspond to maximal anomaly scores, signalling potential fraudulent behaviour. The average path length is measured by estimating the number of edges from the root node to the terminal node for each point over all trees in the forest. This isolation forest function in two stages such as training and testing phases. In the training phase, isolation tress are constructed using only known normal transaction data, proficiently capturing standard behavioural patterns.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025

DOI: 10.17148/IJARCCE.2025.14718

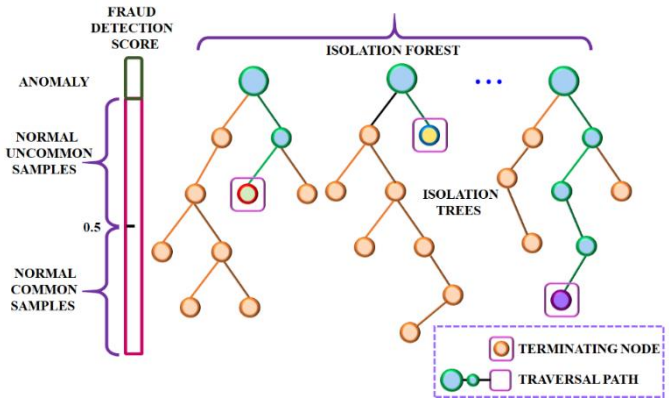

Fig. 3 Fraud prediction based isolation forest model

In the testing phase, every incoming transaction is given via the isolation forest to compute its path lengths and subsequently, its anomaly score. Transactions yield significantly shorter path lengths compared to the learned norms are identified as potential frauds.

IV. RESULTS AND DISCUSSION

The proposed model gets validated in this section by providing the comparative analysis with various classical models. The comparison of various AI-based fraud detection models shows considerable differences in prediction accuracy and error rates as detailed below.

TABLE II COMPARISON OF ERROR METRICS

Methodology	MAE	RMSE
AIDE [28]	0.054	0.171
KNN [18]	0.044	0.209
NB [29]	0.081	0.228
RT [30]	0.048	0.218
Proposed	0.028	0.168

As signified in Table 2, with the lowest MAE of 0.028 and RMSE of 0.168, the proposed model performs better than the others, showing that it is more reliable in reducing prediction errors and more accurate in identifying fraud. This low error rate shows the model generalises over unseen data, which results of sophisticated proposed hybrid model and efficient data preprocessing.

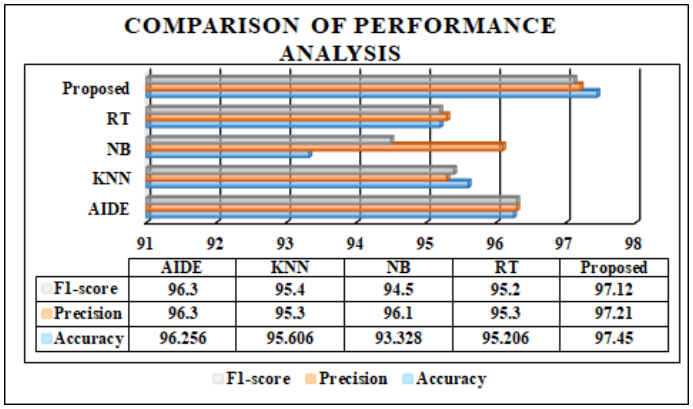

Fig. 4 Comparison of performance analysis

The evaluation metrics such as precision, Accuracy and F1-score are compared with the conventional deployed models, which prove the identity of proposed model for predicting fraud behaviour. As mentioned in Fig. 4, higher evaluation metrics are accomplished by the value of accuracy (97.45%), precision (97.21%) and F1-score (97.12%), correspondingly.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025
DOI: 10.17148/IJARCCE.2025.14718

V. CONCLUSION

A sophisticated AI based hybrid ML model proposed to boost up the fraud detection rate in financial cybersecurity applications. The multi threats data's quality is improved by the preprocessing system, which ensures that the learning model receives high fidelity data for analysis. Moreover, Isolation Forest and rule-based logic in a hybrid detection approach proficiently capture known and undiscovered fraud behaviours. By addressing the main drawbacks a classical models, this combination model allows for high detection accuracy, fewer false positives and more adaptability to changing threat landscapes. The comparative analysis using standard performance evaluation metrics such as MAE, RMSE, validates the effectiveness of proposed model, which accomplishes lowest MAE (Mean Absolute error)of 0,028, RMSE (Root Mean Square error) of 0.168 with higher accuracy, precision and F1-score, thereby overtaking classical models. These outcomes confirm that with the assistance hybrid ML model detecting fraud precisely with higher accurate solution, thereby securing financial systems against conventional fraud threats.

REFERENCES

[1]. O. Olowu, A. O. Adeleye, A. O. Omokanye, A. M. Ajayi, A. O. Adepoju, O. M. Omole, and E. C. Chianumba, "AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity," 2024.
[2]. A. M. Ajayi, A. O. Omokanye, O. Olowu, A. O. Adeleye, O. M. Omole, and I. U. Wada, "Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity," 2024.
[3]. K. Venigandla, and N. Vemuri, "RPA and AI-driven predictive analytics in banking for fraud detection," *Tuijin Jishu/Journal of Propulsion Technology*, vol. 43, no. 4, 2022.
[4]. I. A. Salami, A. Deborah Popoola, M. O. Gbadebo, F. H. Oluwapamilerin Kolo, and T. O. Adesokan-Imran, "AI-Powered Behavioural Biometrics for Fraud Detection in Digital Banking: A Next-Generation Approach to Financial Cybersecurity," *Asian Journal of Research in Computer Science,* vol. 18, no. 4, pp. 473-494, 2025.
[5]. A. Wahid, K. Ali, "AI-Driven Fraud Detection: Strengthening Cybersecurity in Finance and Ensuring Ethical Considerations," 2025.
[6]. P. Raghuwanshi, "AI-Driven Identity and Financial Fraud Detection for National Security," *Journal of Artificial Intelligence General Science (JAIGS)*, vol. 7, no. 01, pp. 38-51, 2024.
[7]. M. M. Islam, I. Zerine, M. A. Rahman, M. S. Islam, and M. Y. Ahmed, "AI-Driven Fraud Detection in Financial Transactions–Using Machine Learning and Deep Learning to Detect Anomalies and Fraudulent Activities in Banking and E-Commerce Transactions," 2024.
[8]. M. Z. Islam, S. K. Shil, and M. R. Buiya, "AI-driven fraud detection in the US financial sector: Enhancing security and trust," *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence,* vol. 14, no. 1, pp. 775-797, 2023.
[9]. S. Thapaliya, "Examining the Influence of AI-Driven Cybersecurity in Financial Sector Management," *The Batuk,* vol. 10, no. 2, pp. 129-144, 2024.
[10]. B. Johnson, "Artificial Intelligence and Cybersecurity in Banking Sector: Opportunities and Risks," 2025.
[11]. S. Kalisetty, C. Pandugula, L. R. K. Sondinti, G. Mallesham, and PR S. Rani, "AI-Driven Fraud Detection Systems: Enhancing Security in Card-Based Transactions Using Real-Time Analytics," *Journal of Electrical Systems*, vol. 20, pp. 1452-1464, 2024.
[12]. L. L. Scientific, "AI-Driven Fraud Detection and Security Solutions: Enhancing Accuracy in Financial Systems," *Journal of Theoretical and Applied Information Technology*, vol. 103, no. 8, 2025.
[13]. H. O. Bello, A. B. Ige, and M. N. Ameyaw, "Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments," *World Journal of Advanced Engineering Technology and Sciences,* vol. 12, no. 02, pp. 021-034, 2024
[14]. A. Mohammed, "Fraud Detection in Banking Data by Machine Learning Techniques," 2025.
[15]. X. Lei, U. H. Mohamad, A. Sarlan, M. Shutaywi, Y. I. Daradkeh, and H. O. Mohammed, "Development of an intelligent information system for financial analysis depend on supervised machine learning algorithms," *Information Processing & Management*, vol. 59, no. 5, pp. 103036, 2022.
[16]. S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud detection in banking data by machine learning techniques," *IEEE Access*, vol. 11, pp. 3034-3043, 2022.
[17]. B. Narsimha, C. V. Raghavendran, P. Rajyalakshmi, G. Kasi Reddy, M. Bhargavi, and P. Naresh, "Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application," *International Journal of Electrical and Electronics Research,* vol. 10, no. 2, pp. 87-92, 2022.
[18]. J. Ren, X. Liu, Q. Wang, H. He, X. Zhao, "An multi-level intrusion detection method based on KNN outlier detection and random forests", *J. Comput. Res. Dev*., vol. 56, pp. 566–575, 2019.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 7, July 2025

DOI: 10.17148/IJARCCE.2025.14718

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

[20]. H. Du, L. Lv, A. Guo, and H. Wang, "AutoEncoder and LightGBM for credit card fraud detection problems," *Symmetry*, vol. 15, no. 4, pp. 870, 2023.

[21]. A. K. Veldurthi, "The Role of AI and Machine Learning in Fraud Detection for Financial Services," *Journal of Computer Science and Technology Studies*, vol. 7, no. 4, pp. 757-771, 2025.

[22]. F. T. Johora, R. Hasan, S. F. Farabi, J. Akter, and M. Abdullah Al Mahmud, "AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions," *The American journal of management and economics innovations*, vol. 6, no. 06, pp. 8-22, 2024.

[23]. A. Mutemi, and F. Bacao, "E-commerce fraud detection based on machine learning techniques: Systematic literature review," *Big Data Mining and Analytics,* vol. 7, no. 2, pp. 419-444, 2024.

[24]. M. B. Ndirangu, and A. Matheka, "A Hybrid Model for Detecting Insurance Fraud Using K-Means and Support Vector Machine Algorithms," *Open Journal for Information Technology,* vol. 6, no. 2, pp. 143, 2023.

[25]. P. Elechi, and I. O. Abasi Michael, "Enhanced predictive data mining algorithm for fraud detection and churn behaviour modelling in telecommunication systems."

[26]. R. Dey, A. Roy, J. Akter, A. Mishra, and M. Sarkar, "AI-driven machine learning for fraud detection and risk management in US healthcare billing and insurance," *Journal of Computer Science and Technology Studies,* vol. 7, no. 1, pp. 188-198, 2025.

[27]. F. A. Bakare, O. J. Ikumapayi, "Securing Government Revenue: A Cloud-Based AI Model for Predictive Detection of Tax-Related Financial Crimes."

[28]. B. Khan, R. Naseem, M.A. Shah, K. Wakil, A. Khan, M. I. Uddin, M. Mahmoud, "Software Defect Prediction for Healthcare Big Data: An Empirical Evaluation of Machine Learning Techniques", *J. Healthc. Eng*., pp. 8899263, 2021.

[29]. U. Purwar, S. Gupta, V. Gautam, S. C. Maurya, "A comparative analytics of SVM DT NB classifier for heart disease prediction in MLalgorithms", *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 5, pp. 3117–3120, 2023.

[30]. R. Naseem, B. Khan, A. Ahmad, A. Almogren, S. Jabeen, B. Hayat, M.A. Shah, "Investigating Tree Family Machine Learning Techniques for a Predictive System to Unveil Software Defects", *Complexity*, pp. 6688075, 2020.