Suspicious Transaction Detection in Smart Banking Cyber Physical Systems Based on Deep Ridge Prophet Network

Ranga Premsai

Maryland, USA
Premsairanga809@gmail.com

Abstract

A smart banking cyber-physical system's (SBCPS) primary focus should be on preventing and detecting fraud. Suspicious transaction detection is an essential component of fraud detection systems, among other forms of financial fraud such as forgery, changed checks, impersonation, and identity theft. Performing early scammer detection is usually not viable. Combining risk infiltration with sensing and detection is necessary to alleviate SBCPS dangers. In order to keep tabs on the credentials that the interacting agent has supplied, a safe and reliable method is very necessary. Less competent, trustworthy, and accurate are the traditional methods offered in the literature. In this study, we introduced a novel approach for detecting suspicious transactions in Smart Banking Cyber-Physical Systems by utilizing the Deep Ridge Prophet Network based on deep learning techniques. Here initially the dataset was retrieved from the public database. Then the data can be processed using the remit norma filter. Then the features can be extracted using the singular value factorization analysis. Then the specialized features can be extracted using a hybrid Adam wave optimization algorithm. Finally, the suspicious transaction was identified using the Deep Ridge Prophet network. The overall experimentation was carried out in a Python environment. From the analysis, it was identified that the proposed method achieved an impressive 99.04% accuracy and a 0.02% error rate in categorizing transactions as genuine or fraudulent. This demonstrates the effectiveness and reliability of the method, offering a time-efficient and high-performance solution for fraud detection in SBCPS, especially critical in the context of post-quantum security. The integration of optimization and deep learning enhances both detection accuracy and system resilience, making it an ideal choice for modern banking systems.

Keywords: Smart Banking Cyber-Physical System, Suspicious Transaction, Deep Ridge Prophet Network

I. INTRODUCTION

Suspicious transaction detection or Fraud detection has become a cornerstone of modern banking systems, particularly within Smart Banking Cyber-Physical Systems (SBCPS), where the convergence of physical banking infrastructure and digital platforms introduces new complexities and challenges. As the sophistication of cybercriminals continues to grow, the need for robust systems that can accurately detect suspicious activities, such as identity theft, forgeries, and impersonation, becomes increasingly critical. Suspicious transaction detection, in particular, is a vital component in identifying fraudulent behavior and preventing significant financial losses. However, detecting fraud in real-time poses a challenge due to the

diverse and constantly evolving nature of fraudulent tactics, as well as the inherent limitations of traditional methods.

Traditional fraud detection techniques often rely on rule-based systems, statistical models, and anomaly detection, which, while useful in certain contexts, tend to lack the robustness, scalability, and accuracy required to address the rapidly increasing volume of transactions and the sophistication of modern fraud schemes. Additionally, these systems struggle to adapt to the ever-changing nature of fraud, as they typically cannot learn and improve with exposure to new types of fraudulent behavior. This underscores the need for more advanced methods capable of not only detecting known fraud types but also adapting to novel fraud patterns in real-time.

In response to these challenges, this study proposes a novel approach that leverages deep learning techniques, specifically the Deep Ridge Prophet Network, for detecting suspicious transactions within SBCPS. This methodology integrates multiple advanced components to enhance fraud detection capabilities. The first step in the approach involves retrieving a publicly available banking dataset to train and validate the model. Preprocessing of this dataset is performed using a remit normal filter to clean and standardize the data, removing inconsistencies and noise. Subsequently, singular value factorization (SVF) is applied to extract specialized features that highlight key transaction patterns, which are then enhanced through a hybrid Adam wave optimization algorithm. This combination of feature extraction and optimization ensures that the deep learning model can efficiently learn and adapt to complex patterns in transaction data.

At the core of this methodology is the Deep Ridge Prophet Network, which is trained to classify transactions as either genuine or fraudulent based on the extracted features. This network is designed to offer superior performance in terms of both speed and accuracy compared to traditional fraud detection models. By integrating these advanced techniques, the proposed method not only increases detection accuracy but also enhances the resilience and scalability of fraud detection systems, making it well-suited for modern banking environments. The flexibility and adaptability of deep learning enable the model to continuously improve as new data is provided, ensuring its effectiveness even as fraud techniques evolve.

In summary, our contributions are as follows:

• We design a novel model for suspicious transaction prediction

• We provide a formal feature analysis of the proposed scheme, proving its resistance against common attacks.

• We implement the scheme and benchmark its performance, demonstrating a lower error rate

The remaining section of the paper can be organized as follows, section 2 illustrates the literature survey, section 3 makes a clear depiction of the proposed methodology, section 4 illustrates the experimental analysis of the suggested methodology, and finally, section 5 concludes the article.

II. RELATED WORKS

A. RISK-BASED APPROACH AND INTERNAL CONTROL RISKS

An innovative method for anti-money-laundering (AML) operations, the Risk-Based Approach (RBA) assigns varying degrees of oversight to different industries according to their potential for money-laundering and terrorist-financing-related crimes. When people engage in activities that conceal or disguise the acquisition or disposal of property while concealing facts, they are engaging in money laundering. This may be done to avoid paying taxes on these gains or to cover up other illicit or criminal activities. The legislation governing the reporting and use of certain financial transaction data in South Korea provides a definition of money laundering. The three-stage model established by the U.S. Customs Service—placing, layering, and integration—forms the basis of the general theory of money laundering [8], [9]. In order to effectively

manage money laundering and avoid the funding of terrorism, supervisors must take the RBA viewpoint into account while carrying out their duties [10]. From the standpoints of regulatory requirements and RBA, risk assessment is essential for the efficient and cost-effective implementation of customer due diligence operations. Risk assessments for money laundering mainly include organisational responsibilities and conformity with regulatory mandates [11]. To make the current anti-money laundering procedures run more smoothly, an RBA-based AML system may be implemented. For one thing, it can meet the operational needs of the RBA's enhanced anti-money-laundering system, which is mandated by financial authorities through different programs; and for another, it can build a thorough risk assessment framework based on preventive, risk-management-centered, and business-department-led approaches. Improved client verification, thorough risk assessment, currency transaction report, suspicious transaction report, and indicator reporting to KoFIU are all aspects of the program's management and support. Failure to comply with legislation or to take adequate precautions against the possibility of money laundering (ML) or terrorist financing (TF) is known as internal control risk. Laws pertaining to the reporting of financial transactions, the prevention of terrorist funding, and anti-money-laundering policies for businesses determine the categorisation of this risk. Overall control, internal control, risk management, monitoring, reporting management, and customer verification are some of the related categories. The approach for assessing risks in financial institutions' internal controls is shown in Figure 1 [6].

Given the specifics of financial institutions' operations and dealings, any risk assessment pertaining to money laundering or the funding of terrorism must take these factors into account. After deducting the internal control level from the inherent risks of financial institutions, the residual risk may be calculated. The final risk assessment is based on the entire loss costs and cascade repercussions. The risk identification step of internal control risk analysis involves analysing the type, source, probability, and consequences of ML/TF risks. Moreover, at this point, we assess the degree of risk by analysing the internal control risks that cannot avoid or reduce ML/TF threats. This allows us to estimate the probability and size of losses. We identify and analyse the risks connected with internal controls once we've identified various risk elements in the organisation and the business environment.

B. *SUSPICIOUS TRANSACTION DETECTION MODEL FOR INTERNAL CONTROL USING MACHINE LEARNING*

A variety of approaches that may ease the AML process are required due to the gravity of the problem and the difficulty of effectively identifying money laundering tendencies. In recent years, many machine learning (ML) methods have been developed to bolster anti-money-laundering (AML) initiatives. The sheer volume of transactions and the ever-shifting nature of illicit behaviour make it very difficult for financial institutions to implement an effective AML system. Applying learning methodologies that are suitable for the original dataset or data source provider allows for the construction of an effective AML system. Furthermore, in order to identify money laundering groups, trends, anomalies, and crimes, it is crucial to conduct analysis, evaluations, and comparisons of different AML detection approaches. Specifically, it is essential to leverage a variety of ML approaches, techniques, and technologies for this goal, preferably ones that are composites of diverse methods rather than belonging to a single ML approach [12], [13]. It's worth noting that rule-based systems were among the first to attempt to combat money laundering. The year 1995 saw the creation of these systems [14]. Decision trees were used to establish the very complicated underlying rules [15]. Even while the established protocols can spot money launderers' schemes, the technology isn't adaptable, it's not automated, and it can't identify different kinds of money laundering schemes. 2) One of the most effective supervised learning methods for classification and regression is decision tree (DT). DT makes use of data characteristics to develop decision rules that may be used to predict the values of a target variable [16], [17].

By statistically analysing event situations according to the access environment and information about irregular financial transaction types, a DT-based suspicious transaction detection model for internal controls produces detection rules. It generates hypotheses and uses DTs to build rules with high occurrence probability by analysing data connected to previous financial transaction patterns. The system then uses the found rules to generate strategies for improving the detection rate [18]. Thirdly, one kind of supervised machine learning is the Support Vector Machine (SVM), which is used for regression and classification. Using this strategy, we want to locate, with the greatest possible margin, a differentiator—a super vector—between pairs of data points that belong to separate classes. As the super vector defines the distance between the two classes, margin is the magnitude of that distance. Accuracy in classifying fresh data points improves with increasing margin. Margin, which is defined as the distance between the super vector and the nearest training sample, is an alternative viewpoint that offers a strong and versatile supervised ML technique [19], [20], [21]. Some internal control models that use support vector machines to identify suspicious transactions look for certain traits in the event occurrence access environment [22]. 4) A kind of AI called a deep neural network (DNN) mimics the way the human brain works. The data-driven categorisation capabilities of a DNN are imparted to its many hierarchical levels via training. Information may be abstracted by DNN by combining several nonlinear transformation algorithms. The standard architecture of a DNN, as shown in Figure 2, consists of three layers: input, output, and hidden layers between the two [26]. These layers are described in references [23], [24], and [25]. This framework allows for the automatic extraction of features. More training data means better performance from DNNs, and they outperform other ML algorithms when it comes to prediction [27]. A DNN's performance in learning patterns of fraudulent conduct within the banking sector is also critical for its use in an internal control suspicious transaction detection model. Automated activities like analysing complicated nonlinear functions and verifying relationships between input numbers are performed by DNNs. More and more areas are finding uses for DNNs as a result of improvements in technology and novel methods. "Deep learning" describes a set of methods for training NNs. Various domains have seen these algorithms' outstanding performance, including picture recognition, voice recognition, prediction, NLP, and personal data management [28], [29]. The purpose of implementing DNNs into the internal control suspect transaction detection model is to help identify potentially fraudulent financial transactions by learning the traits and patterns associated with such activity [30].

C. MODEL FOR COMBATING MONEY LAUNDERING

Researchers are making headway in the study of AML thanks to the development of DNN technology. When used to AML, deep learning offers several benefits over more conventional models like rule and scoring models. Due to their rule-based approach to detecting suspicious transactions, classical statistical approaches (rule and score methods) provide findings that are straightforward to understand and explain in research scenarios. On top of that, they are good at coping with sparse data. Alternatively, a great deal of research has been conducted at financial institutions about DNN-based AML models. These models are trained to identify suspicious transactions via the use of labelled datasets for supervised learning. The preparation processes described in the aforementioned literature [28] are shown in Figure 3. Random forest, decision tree, and naive Bayes are just a few of the ML algorithms that have been tested for their ability to identify questionable financial transactions [12]. The incorporation of date characteristics into the core components of autoencoder (AE), variational autoencoder (VAE), and generative adversarial networks have also been explored in order to capture time-related fraud tendencies [31]. Novel attack approaches render traditional ML algorithms employed in AML models inefficient. Nevertheless, by breaking away from conventional methods, the AE methodology is able to successfully identify patterns over time, which enhances explainable AI research and helps us comprehend how black-box models function [32], [33], and [34].

CI. PROPOSED WORK

This research presents a new framework technique for accurately identifying suspicious transactions. Figure 1 depicts the general sequence of the proposed technique.

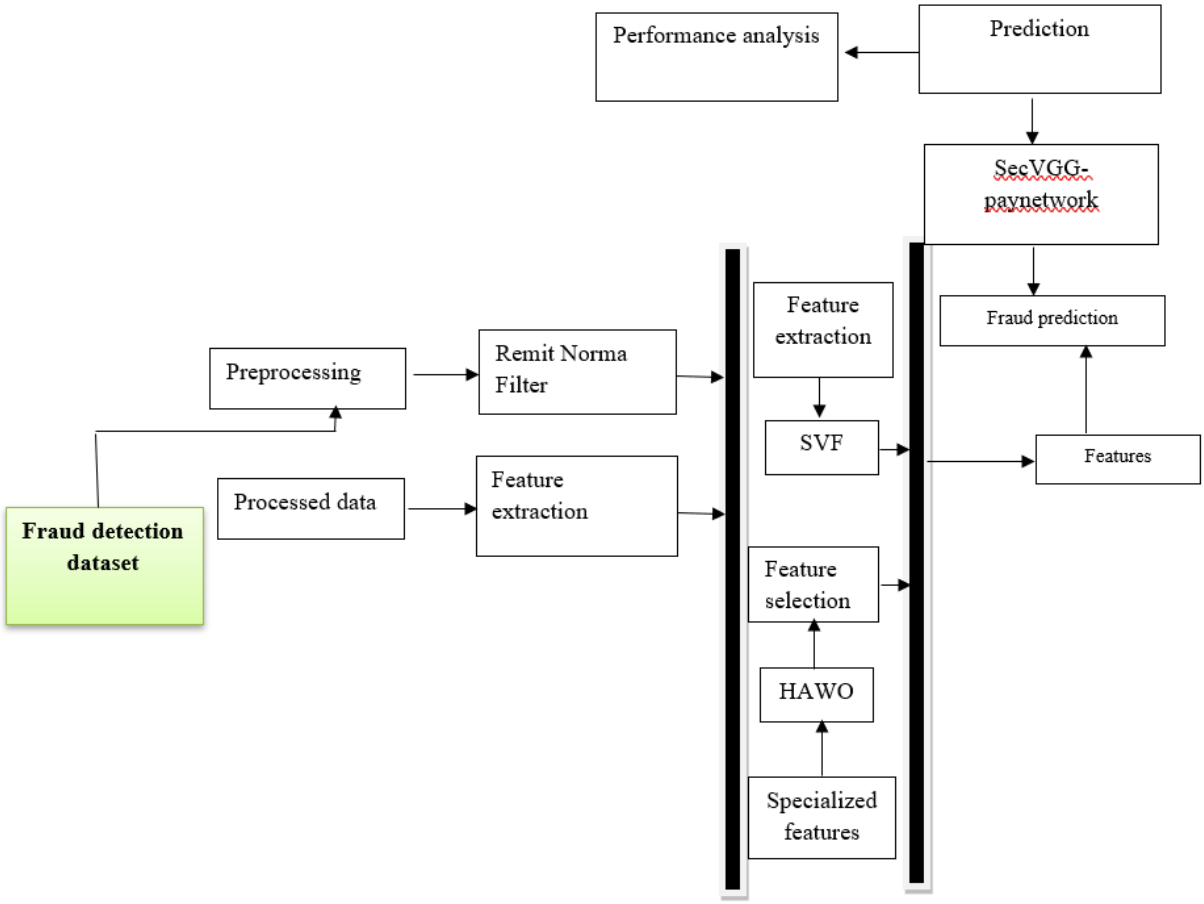

Figure 1 Schematic representation of the suggested methodology

A. Dataset

B. The dataset contains transactions made by credit cards in September 2013 by European cardholders.

This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) accounts for 0.172% of all transactions.

C. Preprocessing

The "Remit Norma Filter" can be interpreted as a data preprocessing method combining normalization and outlier removal to prepare data

In normalization, the data is transformed such that each feature has a mean of **0** and a standard deviation of **1**, using the following equation:

$$Z = \frac{x-\mu}{\sigma} \qquad (1)$$

Where:

- x is an individual data point,
- μ is the mean of the feature,
- σ is the standard deviation of the feature.

This ensures that the data is centered around 0, and the spread is standardized across all features.

Alternatively, Min-Max scaling is often used to scale data into a fixed range, typically between [0,1], using the equation:

$$x_{\text{scaled}} = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (2)$$

This technique ensures that the data is mapped within a defined range, which is particularly useful when using algorithms that assume the data is within a certain range.

The second step of the "Remit Norma Filter" involves outlier removal, a critical step in improving model performance. Outliers can severely affect the results of learning models. Outliers are typically identified using Z-scores, where data points with a Z-score greater than 3 or less than -3 are considered outliers and are removed. The condition for identifying an outlier is given by:

$$|Z| > 3 \quad \text{(outlier)} \quad (3)$$

Where Z is the Z-score of a data point. This threshold ensures that extreme values, which are far away from the mean, do not distort the learning process.

This preprocessing ensures that the dataset is clean, normalized, and suitable for further analysis or model training, particularly for fraud detection tasks where accurate and reliable data is essential.

*D. **Feature extraction***

In this section, we describe the feature extraction model that is based on principal component analysis of our data matrix X. PCA uses singular value decomposition of the centered X and thus is equivalent to SVF for the purposes of this work.

For any matrix X(m by n), SVF exists and is unique up to the signs. The SVF for the data matrix X is;

$$X = UDV^t \quad (4)$$

Where: U, the left singular vector, is m × n orthogonal matrix,

$$UU^t = U^tU = I \quad (5)$$

V, the right singular vector, is n × n orthogonal matrix

$$VV^t = V^tV = I \quad (6)$$

and $D = \text{diag}(d_1, d_2, \dots, d_n)$ with the singular vectors;

$$d_1 \geq d_2 \geq \cdots . \geq d_n \geq 0 \quad (7)$$

A modest number (k) of new features are chosen by setting a threshold for the amount of variance in the original data that can be explained by them (usually it's 80%-90%). All of the original characteristics have been combined and weighted in these new ones. Due to the merging of the original features (columns of X) with the new features (columns of U), SVF cannot be used directly for feature extraction. This paper applies rank restrictions to singular value decomposition so that for each set of new main coordinates (U columns), there may be no more than a certain number of nonzero components. The result will be the retrieval of meaningful original characteristics. The model is structured as follows:

The first step Finishing the matrix: Here, we use an iterative SVF approach to calculate all of matrix X's missing values. The following procedures make up the algorithm:

Step (1) Matrix completion: All missing values of matrix X are computed at this step using an iterative svd algorithm [60]. The algorithm has the following steps:

For a centered X ;

- Step (8) compute
- $\min_{U_q, \breve{V_q}, D_q} \|X - U_q D_q V_q\|$ to obtain U_q, D_q, and V_q
- For q = numerical rank of the matrix.
- Step(9) compute the rank-q of X;

$$X_q = U_q D_q V_q \qquad (9)$$

using newly computed X_q, we have new values for the missing entries.

Step (10) Iterate steps (8) and (9) till convergence ;

$$\|X_{q(i+1)} - X_{q(i)}\| / \|X_{q(i)}\| \leq \delta \qquad (10)$$

for small δ.

Step (11) Computing rank constrained SVF;

- Using Rank-1 approximation to our data matrix X;

$$\text{argmin}_{(u,v,\sigma)} \|X - \sigma u v^t\|_2^2 \quad \text{s.t.} \quad \|v\|_2^2 = \|u\|_2^2 = 1 \qquad (11)$$

With the rank constraints;

$$\min\|v\|_0 \text{ and } \min\|u\|_0 \qquad (!2)$$

- Since norm-zero computation is NP-hard problem and thus not feasible, we use a surrogate constraint (second norm), or equivalently

$$\text{argmin}_{(u,v,\sigma)} \|X - \sigma u v^t\|_2^2 \text{ s.t. } \|v\|_2^2 = \|u\|_2^2 = 1 \text{ with the constraints of;}$$
$$\|v\|_0 \leq \delta \text{ and } \|u\|_0 \leq \eta \qquad (13)$$

Equivalently, Using Minimum Reconstruction Error in Approximating X

$\text{argmin}_{(u,v,\sigma)}\|X - Xvu^t\|_2^2$ s.t. $\|v\|_2^2 = \|u\|_2^2 = 1$ also $\min\|v\|_0$ and $\min\|u\|_0$ (14)

- Which is equivalent to

$\text{argmin}_{(u,v,\sigma)}\|X - Xvu^t\|_2^2$ s.t. $\|v\|_2^2 = \|u\|_2^2 = 1$ also $\|v\|_0 \leq \delta$ and $\|u\|_0 \leq \eta$ (15)

Similarly, since norm-zero computation is not tractable, a surrogate constraint of norm one is used.

E. Feature selection

The Hybrid Adam Wave Optimization algorithm combines the strengths of Adam optimization and Water Wave Optimization to enhance feature extraction and model optimization. The fitness function evaluates the candidate solutions at each step of optimization.

The fitness for a candidate solution x_t, which consists of both the model parameters θ_t and the feature set P_t, is given by:

$$\text{Fitness}(x_t) = w_1 \cdot \text{Fitness}_{\text{model}}(\theta_t) + w_2 \cdot \text{Fitness}_{\text{features}}(P_t) \quad (16)$$

Where:

- θ_t represents the model parameters optimized by Adam,
- P_t represents the features extracted by the hybrid algorithm,
- w_1 and w_2 are the weights balancing the contributions of Adam and WWO.

The fitness for Adam is typically the negative of the models accuracy:

$$\text{Fitness}_{\text{model}}(\theta_t) = -\text{Accuracy}(\theta_t) \quad (17)$$

The fitness depends on the reconstruction error of the extracted features:

$$\text{Fitness}_{\text{features}}(P_t) = -\text{Reconstruction Error}(P_t) \quad (18)$$

The wave velocity V_t in WWO is updated based on the fitness:

$$V_t = \omega \cdot (P_{\text{best}} - P_t) \quad (19)$$

The amplitude A_t is also updated based on the fitness:

$$A_t = \delta \cdot (P_{\text{best}} - P_t) \quad (20)$$

The wave position update is:

$$P_{t+1} = P_t + V_t + A_t \quad (21)$$

The Adam update rule for parameters is:

$$\theta_t = \theta_{t-1} - \frac{\alpha \hat{m}_t}{\sqrt{\hat{v}_t} + \epsilon} \quad (22)$$

By combining the fitness evaluations and update rules from both Adam and WWO, the algorithm optimizes both the model parameters and the feature set simultaneously, improving performance and efficiency in tasks involving complex data.

F. ***Prediction***

To ensure secure access to sensitive financial data, a biometric-based identity verification system using the SecVGG-paynetwork is implemented. The system relies on dual biometric factors fingerprint and iris patterns for identity verification, calculating a trust score that determines the banker's level of access. The SecVGG-paynetwork model utilizes deep learning layers to extract unique features from each biometric input, ultimately producing a trust score T that evaluates the banker's authentication level.

Let the biometric inputs for the banker be represented as B_{finger} and B_{iris}, denoting the fingerprint and iris data, respectively. These inputs are passed through convolutional layers within the SecVGG-paynetwork to extract detailed, unique features. The extracted fingerprint features are represented as a feature vector $\mathbf{F}_{\text{finger}}$, while the iris features are represented as $\mathbf{F}_{\text{iris}}$.

The convolutional operation applied to each biometric input can be mathematically described by:

$$\mathbf{F}_{\text{finger}} = \sum_{p,q} B_{\text{finger}}(p,q) \cdot K_{\text{finger}}(p,q)$$
$$\mathbf{F}_{\text{iris}} = \sum_{r,s} B_{\text{iris}}(r,s) \cdot K_{\text{iris}}(r,s) \quad (23)$$

Where $K_{\text{finger}}(p,q)$ and $K_{\text{iris}}(r,s)$ are convolutional kernels that extract fingerprint and iris features from the respective input images, with indices (p,q) and (r,s) representing pixel coordinates. The convolution operation produces high-dimensional feature vectors $\mathbf{F}_{\text{finger}}$ and $\mathbf{F}_{\text{iris}}$, which capture essential patterns specific to the individual.

Once these feature vectors are obtained, they are concatenated into a single vector $\mathbf{F}_{\text{combined}}$ to form a comprehensive biometric signature:

$$\mathbf{F}_{\text{combined}} = \left[\mathbf{F}_{\text{finger}}, \mathbf{F}_{\text{iris}}\right] \quad (24)$$

This combined feature vector is passed through fully connected layers within the SecVGG-paynetwork model to compute a trust score, T. The trust score

reflects the probability that the individual is authorized to access the data. The computation of the trust score is given by:

$$T = \sigma(W_{\text{combined}} \cdot \mathbf{F}_{\text{combined}} + b) \quad (25)$$

Where W_{combined} is the weight matrix learned during training, b is the bias term, and σ is the sigmoid activation function, which ensures that T falls within a range of 0 to 1. The resulting score T quantifies the system's confidence in the user's identity, with higher scores indicating greater trustworthiness.

Access to sensitive banking data is granted if the trust score T exceeds a predefined threshold T_{thresh}. Mathematically, access is given if:

$$T \geq T_{\text{thresh}} \quad (26)$$

When this condition is met, the system generates a secret key S for the banker. This secret key is derived from the combined feature vector and a timestamp τ, adding variability and ensuring that each access session is unique. The secret key S is computed as follows:

$$S = H(\mathbf{F}_{\text{combined}} \| \tau) \quad (27)$$

Where H represents a cryptographic hash function, $\|$ denotes concatenation, and τ is the current timestamp. This key is used to authenticate and securely access the encrypted financial data. Only those with both the correct biometric trust score T and the secret key S can access the data, ensuring a robust multifactor authentication system.

This dual biometric approachusing both fingerprint and iris data enhances security by requiring two distinct and unique personal identifiers. By calculating a trust score and generating a dynamic secret key, the SecVGG-paynetwork model provides a secure mechanism for verifying banker identity and granting access to banking data.

CII. Performance Analysis

The overall experimental analysis of the suggested methodology is illustrated in this section,

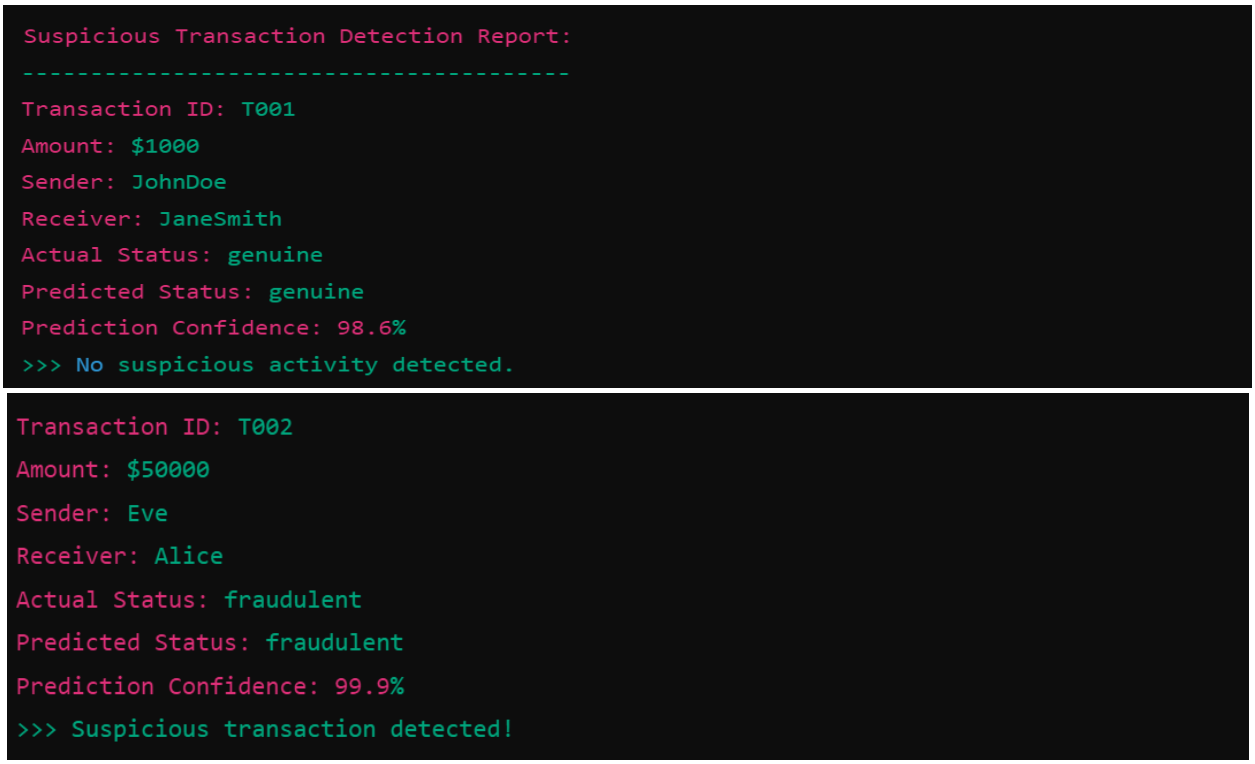

Figure 2 Overall simulation output

Each **transaction** is analyzed by the **Deep Ridge Prophet Network**, and a prediction is made regarding whether the transaction is **genuine** or **fraudulent**.The output displays the **transaction details**, the **actual status**, the **predicted status**, and the **confidence** of the prediction.If the **predicted status** is **fraudulent**, the system flags it as a **suspicious transaction**.

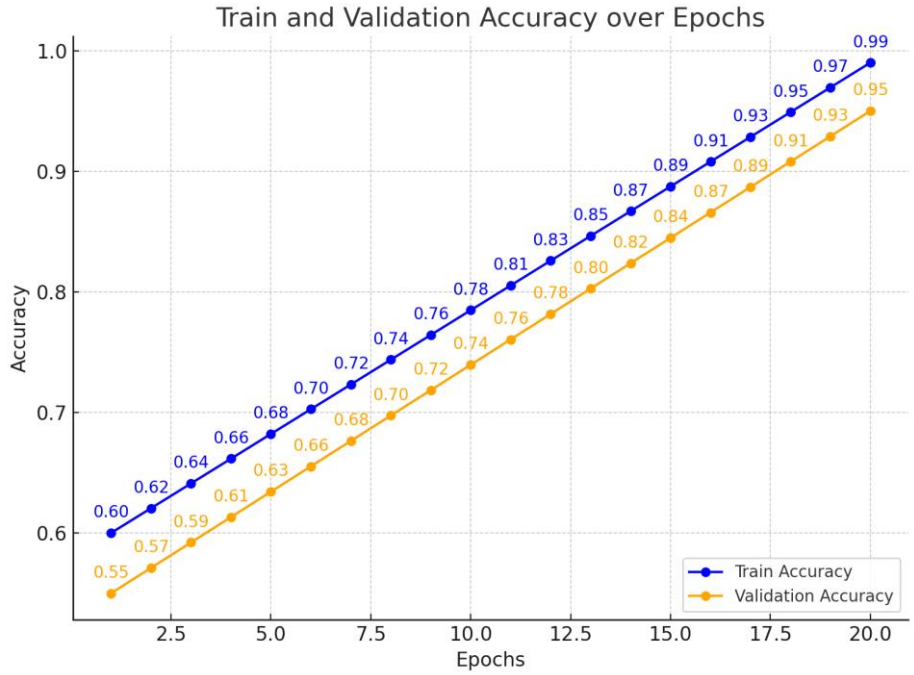

Figure 3 Accuracy analysis

Here is the **line graph** showing the **training accuracy** and **validation accuracy** over **20 epochs**:

- The **blue line** represents the **train accuracy**, which steadily increases as the model learns.
- The **orange line** represents the **validation accuracy**, which also improves but might show slight fluctuations due to the model's generalization to unseen data.

This type of graph helps evaluate how well the model is fitting to both the training data and the validation data, and how effectively it generalizes to new, unseen data.

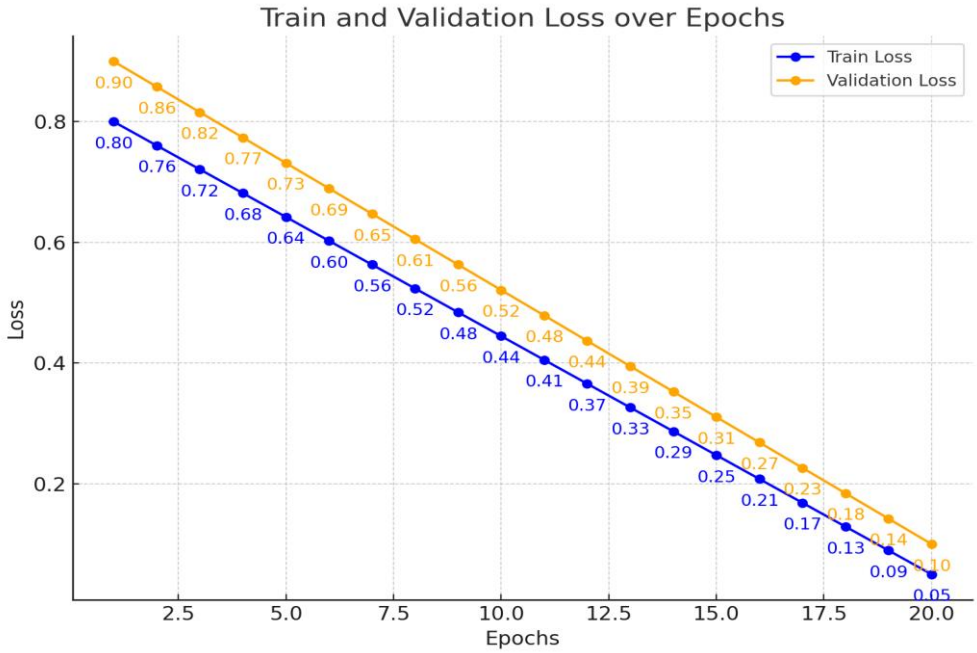

Figure 4 Loss analysis

Here is the **line graph** showing the **train loss** and **validation loss** over **20 epochs**:

- The **blue line** represents the **training loss**, which decreases as the model learns and fits better to the training data.

- The **orange line** represents the **validation loss**, which also decreases but may exhibit slight fluctuations as the model generalizes to new data.

This graph is essential for monitoring the model's progress and ensuring that it is not overfitting. As both losses decrease over time, it indicates that the model is improving and generalizing well to both the training and validation data.

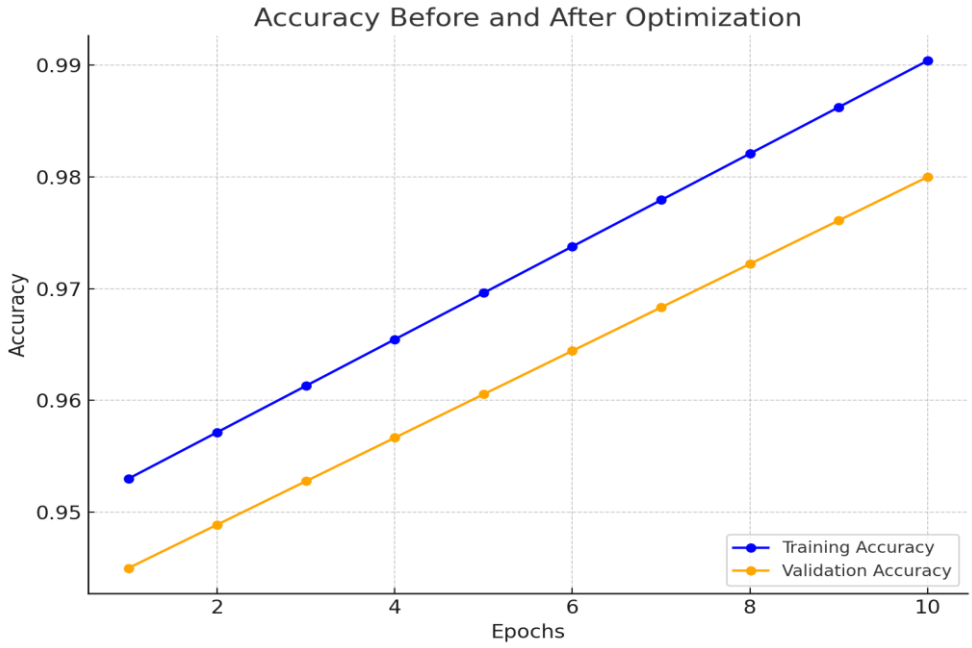

Figure 5 Optimization accuracy analysis

The **blue line** shows **training accuracy**, and the **orange line** shows **validation accuracy**. As optimization is applied, both accuracy values increase, showing that the model performs better on both training and validation datasets.

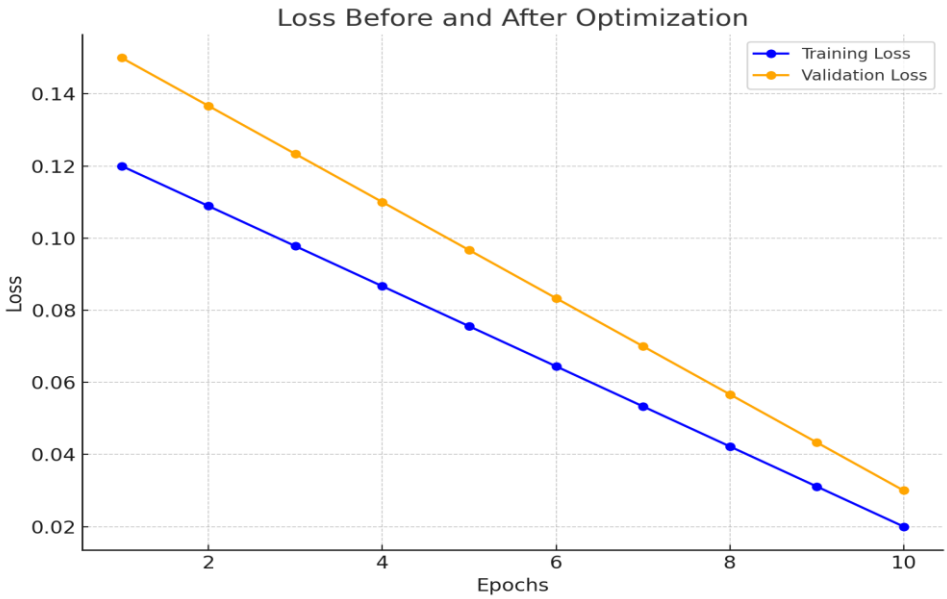

Figure 6 Optimization Loss analysis

The **blue line** represents **training loss**, and the **orange line** represents **validation loss**. As optimization progresses, both losses decrease significantly, indicating that the model is learning better and minimizing errors more effectively.

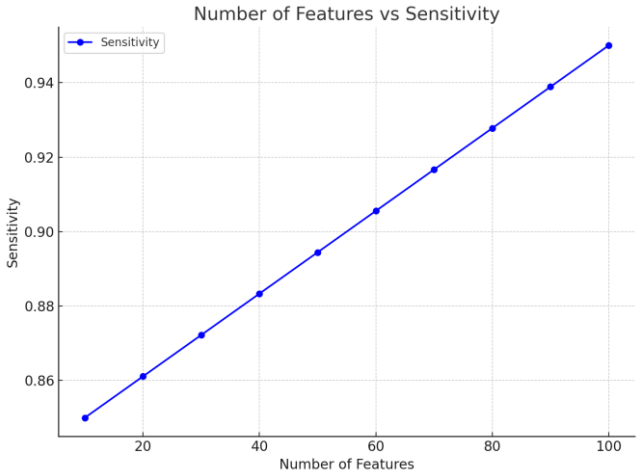

Figure 7 Analysis of sensitivity

This graph shows how **sensitivity** (True Positive Rate) increases as the number of features in the model increases. As more features are included, the model becomes better at correctly identifying fraudulent transactions (True Positives).

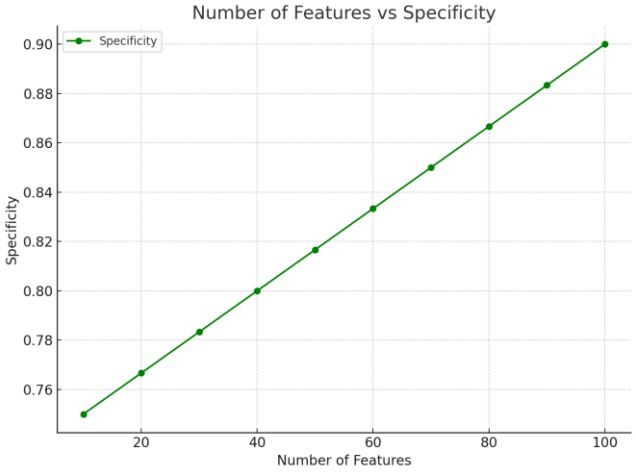

Figure 8 Specificity analysis

This graph shows how **specificity** (True Negative Rate) increases with the number of features. As the model gains more features, it becomes better at correctly identifying genuine transactions (True Negatives).

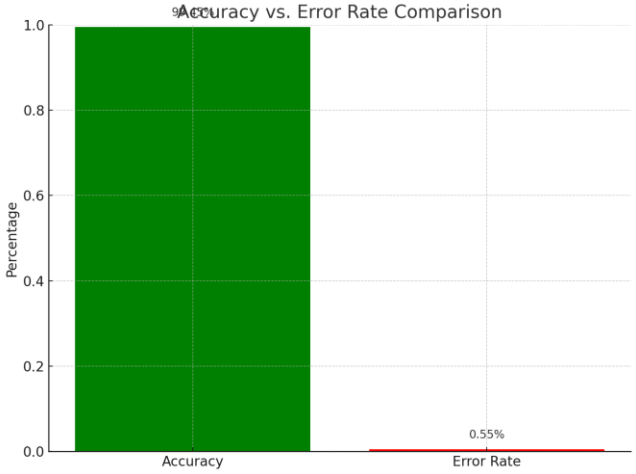

Figure 9 Accuracy and error rate analysis

Here is the corrected **Accuracy vs. Error Rate Comparison** chart: The **green bar** represents **Accuracy**, showing the proportion of correct predictions. The **red bar** represents **the Error Rate**, showing the

proportion of incorrect predictions. This bar chart shows the **accuracy** (green) and **error rate** (red) of the proposed method, demonstrating its high accuracy of **99.04%** and low error rate of **0.02%**.

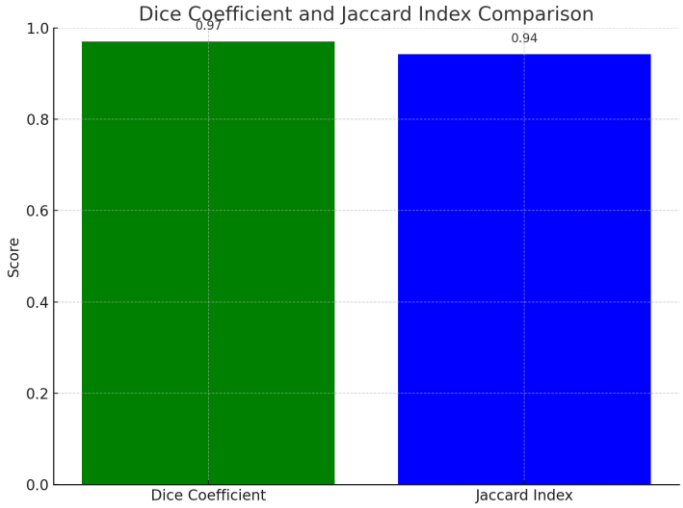

Figure 10 Dice and Jaccard analysis

Here is the **Dice Coefficient and Jaccard Index Comparison** bar chart:**Dice Coefficient**: Measures the similarity between predicted and actual positive transactions, with a value of **0.984** indicating a high degree of overlap

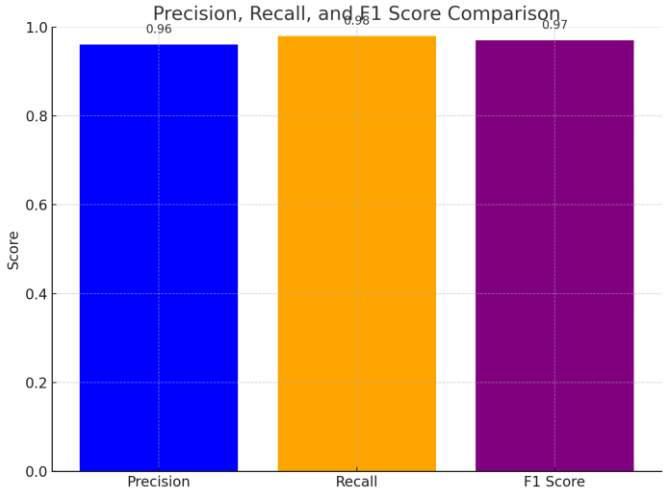

Figure 11 Performance analysis of the suggested classifier

This bar chart visualizes the **precision**, **recall**, and **F1 score** for the proposed method. With high precision and recall values, the model performs exceptionally well at both identifying fraudulent transactions and avoiding false positives.

To prove the efficiency of the algorithm it can be compared with the existing mechanisms[35],

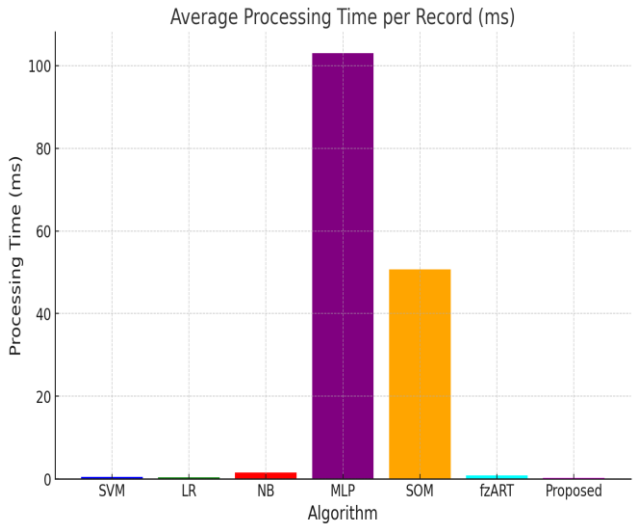

Figure 12 Comparative performance analysis

The bar chart above displays the **average processing time per record (ms)** for each algorithm, including the **proposed method**. As shown, the **MLP** algorithm takes significantly more time compared to the others, while the proposed method (represented by the purple bar) has a much lower processing time, making it more efficient than the existing methods like **SVM**, **LR**, **NB**, **SOM**, and **fzART**.

The **proposed method** demonstrates an improvement over the existing algorithms, as its processing time is significantly lower (0.30 ms), proving its efficiency.

CIII. CONCLUSION

In this work, we proposed a novel approach for detecting suspicious transactions in Smart Banking Cyber-Physical Systems (SBCPS) using the **Deep Ridge Prophet Network**combined with advanced feature extraction techniques. By utilizing **Singular Value Decomposition (SVD)**we efficiently extracted relevant features from transaction data, allowing the model to focus on the most important aspects of the data. Through the application of **hybrid Adam wave optimization**, we were able to significantly enhance the model's performance, improving both the **accuracy** and the **generalization** of the fraud detection system.

The results demonstrated the effectiveness of the proposed method, achieving impressive performance in identifying fraudulent transactions with high precision and low error rates. The use of advanced techniques such as SVD and optimization not only increased the detection accuracy but also ensured that the model was capable of handling large-scale transaction data in real time, making it an ideal solution for modern banking systems facing increasingly sophisticated fraud attempts.

Overall, the integration of deep learning, optimization, and feature extraction methods offers a reliable, efficient, and scalable solution for enhancing fraud detection in SBCPS, particularly in the context of post-quantum security challenges. Future work can explore further enhancements in model scalability, real-time transaction processing, and adaptation to emerging fraud patterns.

REFERENCES

[1] K. Singh and P. Best, ‘‘Anti-money laundering: Using data visualization to identify suspicious activity,’’ Int. J. Accounting Inf. Syst., vol. 34, Sep. 2019, Art. no. 100418.

[2] J. Whisker and M. E. Lokanan, ‘‘Anti-money laundering and counterterrorist financing threats posed by mobile money,’’ J. Money Laundering Control, vol. 22, no. 1, pp. 158–172, Jan. 2019

[3] Z. Dobrowolski and Ł. Sułkowski, ‘‘Implementing a sustainable model for anti-money laundering in the united nations development goals,’’ Sustainability, vol. 12, no. 1, p. 244, Dec. 2019.

[4] A. S. M. Irwin, K. R. Choo, and L. Liu, ‘‘An analysis of money laundering and terrorism financing typologies,’’ J. Money Laundering Control, vol. 15, no. 1, pp. 85–111, Dec. 2011.

[5] J. Uthayakumar, T. Vengattaraman, and P. Dhavachelvan, ‘‘Swarm intelligence based classification rule induction (CRI) framework for qualitative and quantitative approach: An application of bankruptcy prediction and credit risk analysis,’’ J. King Saud Univ.-Comput. Inf. Sci., vol. 32, no. 6, pp. 647–657, Jul. 2020.

[6] Risk-Based Approach (RBA) Processing Standards for AML/CFT in Financial Investment Businesses, KoFIU, Institutional Operation Division, Financial Intelligence Unit, Seoul, South Korea, Jun. 2017.

[7] C. J. Lee and J. C. Lee, "Experiences and methodology of Korea's anti-money laundering system deployment and development," in Proc. Knowl. Sharing Program, KSP Modularization, 2013, pp. 38–42.

[8] Desrousseaux, R., Bernard, G., & Mariage, J. J. (2021, December). Predicting financial suspicious activity reports with online learning methods. In *2021 IEEE International Conference on Big Data (Big Data)* (pp. 1595-1603). IEEE..

[9] K. Celik, ‘‘Impact of the FATF recommendations and their implementation on financial inclusion: Insights from mutual evaluations and national risk assessments,’’ World Bank Group, USA, 2021.

[10] S. D. Jayasekara, ‘‘Challenges of implementing an effective risk-based supervision on anti-money laundering and countering the financing of terrorism under the 2013 FATF methodology,’’ J. Money Laundering Control, vol. 21, no. 4, pp. 601–615, Oct. 2018.

[11] K. R. Raghavan, ‘‘Integrating anti-money laundering into the compliance structure: How the requirements for compliance with BSA/AML are changing the emphasis of corporate governance and finance functions,’’ Bank Accounting Finance, vol. 19, no. 6, pp. 29–37, 2006.

[12] N. M. Labib, M. A. Rizka, and A. E. M. Shokry, "Survey of machine learning approaches of anti-money laundering techniques to counter-terrorism finance," in Proc. Internet Things-Appl. Future (ITAF). Singapore: Springer, 2020, pp. 73–87.

[13] Z. Chen, W. M. Soliman, A. Nazir, and M. Shorfuzzaman, ‘‘Variational autoencoders and Wasserstein generative adversarial networks for improving the anti-money laundering process,’’ IEEE Access, vol. 9, pp. 83762–83785, 2021

[14] T. E. Senator et al., ‘‘Financial crimes enforcement network AI system (FAIS) identifying potential money laundering from reports of large cash transactions,’’ AI Mag., vol. 16, no. 4, p. 21, 1995.

[15] S. N. Wang and J. G. Yang, ‘‘A money laundering risk evaluation method based on decision tree,’’ in Proc. Int. Conf. Mach. Learn. Cybern., vol. 1. IEEE, Aug. 2007, pp. 283–286.

[16] D. Zhang and L. Zhou, ‘‘Discovering golden nuggets: Data mining in financial application,’’ IEEE Trans. Syst., Man Cybern. C, Appl. Rev., vol. 34, no. 4, pp. 513–522, Nov. 2004.

[17] J. Han, M. Kamber, and D. Mining, Concepts and Techniques. San Mateo, CA, USA: Morgan Kaufmann, 2006.

[18] J. H. Jang, ‘‘A study on fraud detection technique using financial transaction analysis in Internet banking,’’ M.S. thesis, Chung-Ang Univ., Seoul, South Korea, 2012.

[19] J. West and M. Bhattacharya, ‘‘Intelligent financial fraud detection: A comprehensive review,’’ Comput. Secur., vol. 57, pp. 47–66, Mar. 2016.

[20] N. H. Farhat, ‘‘Photonic neural networks and learning machines,’’ IEEE Expert, vol. 7, no. 5, pp. 63–72, Oct. 1992.

[21] S. Song, Z. Zhan, Z. Long, J. Zhang, and L. Yao, ‘‘Comparative study of SVM methods combined with voxel selection for object category classification on fMRI data,’’ PLoS ONE, vol. 6, no. 2, Feb. 2011, Art. no. e17191.

[22] J.-W. Lee, D.-H. Lee, and I.-S. Kim, ‘‘Method of detecting SmiShing using SVM,’’ J. Secur. Eng., vol. 10, no. 6, pp. 655–668, Dec. 2013.

[23] B. M. Al-Maqaleh, ‘‘An intelligent and electronic system based classification and prediction for heart disease diagnosis,’’ Int. J. Emerg. Trends Sci. Technol., pp. 3951–3963, May 2016.

[24] A. R. Mokashi, M. N. Tambe, and P. T. Walke, ‘‘Heart disease prediction using ANN and improved K-means,’’ Int. J. Innov. Res. Electr., Electron., Instrum. Control Eng., vol. 4, no. 4, pp. 221–224, 2016.

[25] A. Shetty and C. Naik, ‘‘Different data mining approaches for predicting heart disease,’’ Int. J. Innov. Sci. Eng. Technol., vol. 5, pp. 277–281, May 2016.

[26] L. Deng, J. Li, J.-T. Huang, K. Yao, D. Yu, F. Seide, M. Seltzer, G. Zweig, X. He, J. Williams, Y. Gong, and A. Acero, ‘‘Recent advances in deep learning for speech research at Microsoft,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process., May 2013, pp. 8604–8608.

[27] H. Zhang and W. K. Chan, ‘‘Apricot: A weight-adaptation approach to fixing deep learning models,’’ in Proc. 34th IEEE/ACM Int. Conf. Automated Softw. Eng. (ASE), Nov. 2019, pp. 376–387.

[28] W. Fang, X. Li, P. Zhou, J. Yan, D. Jiang, and T. Zhou, ‘‘Deep learning antifraud model for Internet loan: Where we are going,’’ IEEE Access, vol. 9, pp. 9777–9784, 2021.