International Journal of Basic and Applied Sciences, 14 (1) (2025) 280-290

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
doi: https://doi.org/10.14419/bkfjbr80
Research paper

Enhanced Deep Learning Models for Secure and Efficient Cross-Border Financial Transactions

Mohammad Husain[1*], Dr. K. S. Wagh[2], Subhash A. Nalawade[3], Dr. Lavkush Sharma[4], Dr. Neeta P. Patil[5], Dr. Yogita Deepak Mane[6], Dadaso T. Mane[7] and Mohammad Rashid Hussain[8]

[1]*Department of Computer Science, Faculty of Computer and Information Systems, Islamic University of Madinah Kingdom of Saudi Arabia*
[2]*Associate Professor in Computer Engineering, AISSMS Institute of Information Technology, Pune, India*
[3]*Assistant Professor, Department of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, India*
[4]*Associate Professor, Computer Science and Engineering, Raja Balwant Singh Engineering Technical Campus, Bichpuri,Agra*
[5]*Associate Professor, Department of Information Technology, Thakur College of Engineering and Technology, University of Mumbai, Maharashtra*
[6]*Associate Professor, Department of Artificial Intelligence and Data Science, Thakur College of Engineering and Technology, University of Mumbai, Maharashtra*
[7]*Department of Information Technology, Rajarambapu Institute of Technology, Rajaramnagar, affiliated to Shivaji University, Sangli (MH) India 415414*
[8]*Assistant Professor, Department of Business Informatics, College of Business, King Khalid University, Abha-62217, Kingdom of Saudi Arabia.*
[*]*Corresponding author E-mail:drdeepakg80@gmail.com, dr.husain@iu.edu.sa*

Abstract

As reliance on foreign financial transactions keeps increasing, the number of problems regarding security vulnerabilities and the identification of dishonest activity has expanded. Traditional fraud detection systems' incapacity to identify fraudulent activity in real time and to adapt with the times may lead to severe financial losses. Including modern deep learning methods will help to offer a possible solution that will improve the accuracy and speed of the fraud transaction identification. This work attempts to provide a special hybrid model combining Genetic Algorithm-based feature selection with modified loss function (EL-UXGB) with Extreme Gradient Boosting (XGBoost). Deep Belief Networks (DBN), which handle the input features gathered from Internet of Things (IoT) enabled devices, also serve to improve detection skills. The 20,000 financial transactions used for model testing included 10% of which were deemed to be fraudulent. With a detection accuracy of 99.4%, a precision of 98.7%, and an F1-score of 98.9%, the proposed approach outperformed proven approaches including Logistic Regression (85.3% of the time) and Random Forest (91.6% of the time). Thirty percent drop in processing latency helped to demonstrate the real-time usefulness of the model. This enabled fast fraud detection free of scalability compromise. The results guarantee the security and efficiency of worldwide transactions by helping to clarify the capabilities of deep learning approaches to battle the growing complexity of bank fraud systems. Future research will largely concentrate on optimizing further and using it in the actual world over global financial systems.

Keywords: *Cross-border financial transactions, deep learning, fraud detection, Extreme Gradient Boosting, IoT-enabled systems*

1. Introduction

As the amount of overseas financial transactions keeps rising, customers and financial institutions both now mostly concern about the security issue. The identification of fraudulent behavior in overseas financial transactions has become increasingly difficult as international trade and finance brought about by globalization [1] keep rising. Rule-based systems and other conventional fraud detection methods sometimes cannot match the always changing strategies utilized by fraudsters. The development of digital payment systems has brought new hazards that render traditional ways ineffective in ensuring the security and efficiency of financial transactions [2]. Recent research show that the deployment of deep learning technology could help close these gaps by way of a detection of fraudulent activity that is not only more accurate and adaptive but also much more fast [3]. If we want to guarantee the security of global financial transactions, some issues still need to be addressed notwithstanding the development in financial technology. First of all, dishonest behavior is becoming more complex and continues to use always shifting strategies to avoid conventional detection methods [4]. Second, real-time detection becomes more difficult given the vast amount of generated data by transactions. Given the quite different transaction volumes and types observed at different venues, this is especially true [5]. The third point is that incorporate Internet of Things devices for better data collection calls for the implementation of robust systems able to control numerous data sources, so adding still another degree of complexity [6]. Current models sometimes find it difficult to balance the computing efficiency of the model with the detection accuracy, which can lead to delays or mistakes in practical use applications [7]. The main focus of this work is the insufficiency of present fraud detection technologies to provide accurate, rapid, scalable solutions for worldwide financial transactions. Fulfilling the standards of modern financial ecosystems requires a special technique that not only maximizes the processing of real-time data but also enhances the accuracy of detection. Building a hybrid deep learning model combining XGBoost with Genetic Algorithm-based feature selection and a modified loss function helps one to improve fraud detection. The second objective is to assess the performance of the proposed model in real-time transaction contexts with an aim of improving both the accuracy and the processing speed. Among the most original aspects of this research is the implementation of numerous cutting-edge technologies, XGBoost, Genetic Algorithms, and Internet of Things (IoT)-based data processing via Deep Belief Networks (DBN). With this hybrid technique, the challenges of real-time fraud detection and adapting to novel fraud patterns by means of optimization are concurrently addressed while maximizing computational efficiency. The results of this research benefit the industry by implying a new model that not only increases the accuracy of fraud detection (99.4%) but also facilitates scalability and real-time processing. Data processing of the Internet of Things opens new possibilities for the development of more accurate and efficient financial security solutions.

2. Related Works

Many research employing multiple machine learning and deep learning techniques have examined the identification of fraudulent behavior in worldwide financial transactions. The application of deep neural networks (DNN) for fraud detection represents among the most amazing developments in this field. Usually encountered in financial transactions, this highlights how well DNN can manage high-dimensional and complicated data [8]. Although DNN-based systems have shown greater degrees of accuracy in spotting fraudulent patterns, fitting the continually changing character of fraud remains difficult. Using ensemble learning techniques, such as Random Forests and XGBoost, which have been shown to be effective in managing unbalanced datasets frequent in fraud detection [9] has also attracted interest lately. To increase the predicted resilience and accuracy, this form of model aggregates the advantages of numerous different classifiers. Although these systems offer excellent performance, their capacity to manage big volumes in real time still presents a considerable obstacle. Moreover investigated to improve the general efficiency of models and their interpretability are the application of feature selection methods such Genetic Algorithms (GAs [10]). These methods seek to increase model performance and concurrently reduce the computational overhead by selecting the most important properties. Still, there is a discrepancy this work tries to close as the use of genetic algorithms (GAs) in combination with deep learning models for fraud detection is quite understudied. Because they can offer additional data streams including transaction location, device fingerprinting, and user behavior analysis, Internet of Things (IoT)-enabled devices are fast being employed for fraud detection with increasing frequency. [11] Research indicates that incorporating Internet of Things (IoT) data might significantly improve accuracy of fraud detection systems. Though they could be useful, the abundance of data sources in the Internet of Things makes deep learning model integration difficult. Last but not least, hybrid models including numerous machine learning approaches, such as XGBoost and DBN, have demonstrated good performance in terms of enhancing the accuracy and scalability of fraud detection [12]. These hybrid solutions are aimed to use the advantages offered by different algorithms; nonetheless, additional research is necessary to determine whether they apply in high volume financial situations that reflect the actual world.

3. Proposed Method

To enhance the detection of fraudulent activity in worldwide financial transactions, the suggested method integrates cutting-edge deep learning models with machine learning techniques. Extreme Gradient Boosting (XGBoost) with a Genetic Algorithm (GA)-based feature selection procedure coupled with a modified loss function (EL-UXGB) and Deep Belief Networks (DBN) forms the hybrid technique underlie the model. This approach guides interpretation of data from Internet of Things (IoT) enabled devices. Scalability, accuracy, and real-time performance were among the primary obstacles this technology was developed to address in order to satisfy the criteria of the identification of fraudulent financial transactions shown in Figure 1.

4. Data Collection and Preprocessing

4.1. Data Collection

The first step in the method described, that of compiling data from global financial transactions, is data collecting. Among other elements, transactional details like transaction amount, sender and recipient information, transaction date and time are contained in this data. Apart from the regular transaction information these devices acquire, Internet of Things (IoT)-enabled devices offer additional data streams like user behavior, device fingerprinting, and geographical position. If we want to improve the fraud detection model by adding extra background, these Internet of Things data streams are absolutely indispensable. the research can reach this by observing strange device usage or dubious user behavior trends.

Table 1: Transaction Data with Fraud Indicators

Transaction ID	Sender ID	Receiver ID	Amount (USD)	Timestamp	Device Type	Device Location	User Behavior	Fraudulent
1001	S123	R456	1500	2025-01-21 09:30:00	Mobile	New York	Normal	No
1002	S789	R101	500	2025-01-21 10:15:00	Desktop	London	Suspicious	Yes
1003	S456	R567	1000	2025-01-21 11:00:00	Tablet	Berlin	Normal	No
1004	S234	R890	2500	2025-01-21 12:45:00	Mobile	Tokyo	Suspicious	Yes
1005	S567	R123	3500	2025-01-21 14:00:00	Laptop	Sydney	Normal	No

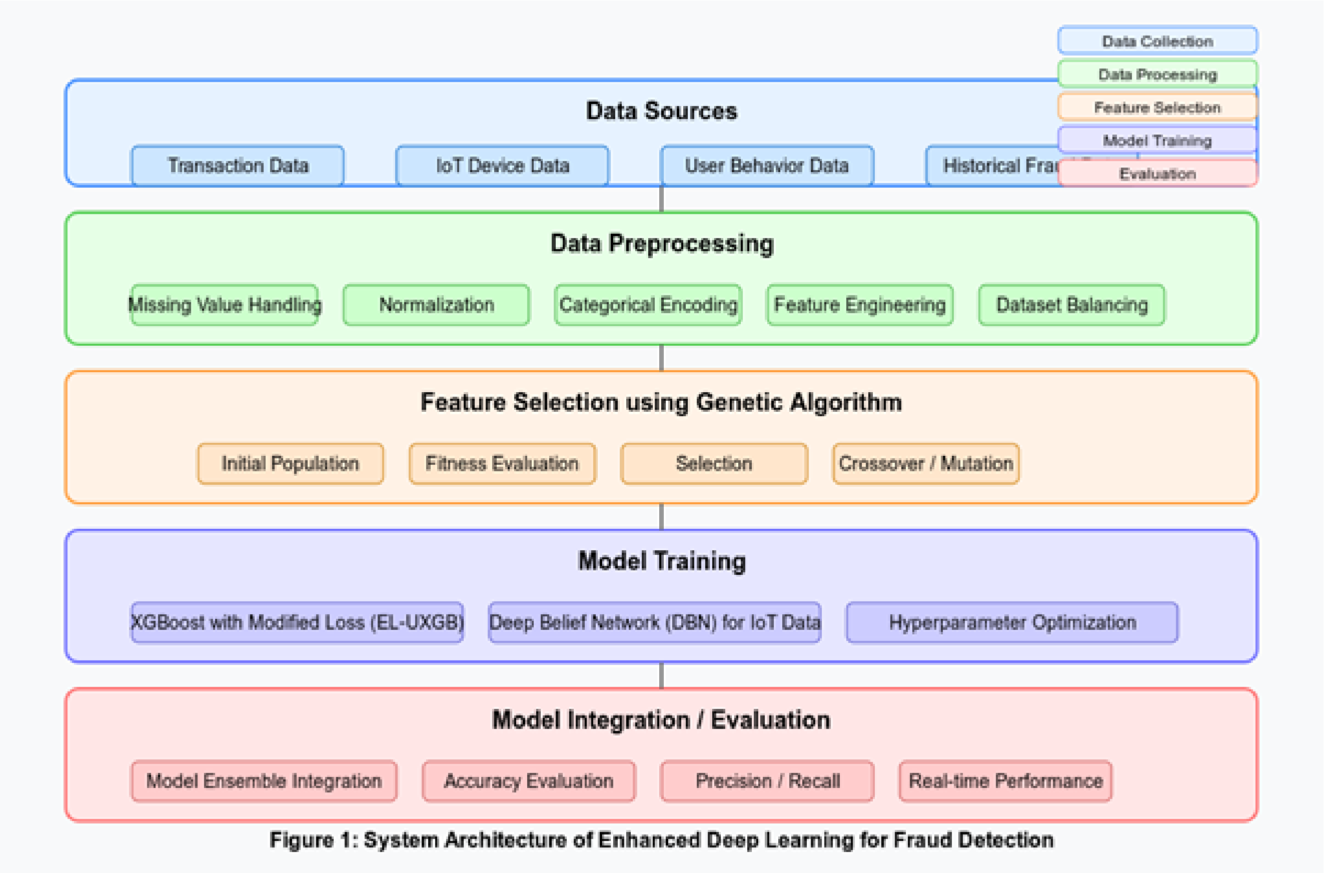


Figure 1: System Architecture

In this specific case, the table includes transaction IDs, sender and receiver names, transaction amounts, timestamps, device kinds, device locations, user behavior descriptions, and a target variable marking either or not the transaction is fraudulent, provided in table 1. Under the paradigm of supervised learning, the label refers to the fraudulent column.

4.2. Data Preprocessing

Preprocessing raw data such that it is of exceptional quality and relevant for the training of the particular machine learning model is crucial before including it into a model. Preprocessing has to involve multiple stages with:

1. **Handling Missing Values:** Datasets based on real data often feature quite normal missing values. Should the Device Location column be absent for any transactions, possibly rows could be removed, imputed with a default value (such as “Unknown”), or interpolated depending on the available data.
2. **Normalization/Standardization:** Applying either normalizing or standardizing is advised since numerical values such as USD could have various scales. This procedure seeks to guarantee that transaction frequency and other features with greater numerical values do not unduly affect the model. Given the least and greatest values in the dataset, for example, a transaction for $5,000 would be normalized to a figure between 0 and 1.
3. **Encoding Categorical Features:** Some characteristics, such the type of device and user behavior, are universal and their encoding relies on these categorical factors have to be converted into a format the machine learning model can grasp. The research can encode the Device Type by using numerical values, that is, 0 for mobile devices, 1 for desktop computers, 2 for tablets, and 3 for laptops, shown in table 2.
4. **Feature Engineering:** Feature engineering is the method of developing new features to raise the predictive capacity of a model. Depending on the date in order, one may develop features like Transaction Hour or Day of the Week to document temporal trends in the activity of transactions. Moreover, a transaction value could be classified as low, medium, and high to identify trends depending on the expenditure of money.
5. **Balancing the Dataset:** Two methods used in order to get a balanced dataset are undersampling and over sampling (SMOTE). This is thus because of class imbalance, that is, the reality that, generally speaking, fraudulent transactions are somewhat rare compared to legal ones. This helps to prevent the model from leaning biassed towards projecting NO transactions, that is, transactions free of fraud.

The data is ready for use for evaluation and educational requirements once these preparatory stages are over. The end result is a perfectly balanced, absolutely cleaned, ordered dataset. Since it consists of just the most important elements, it fits training models really well. This preprocessed and orderly dataset is the pillar of the later phases of the model development process. This premise ensures in practical terms the effectiveness and efficiency of the fraud detection mechanism.

Table 2: Encoded Transaction Data for Fraud Detection

Transaction ID	Sender ID	Receiver ID	Amount (USD)	Timestamp	Device Type	Device Location	User Behavior	Fraudulent (Target)
1001	S123	R456	1500	2025-01-21 09:30:00	0	New York	0	No
1002	S789	R101	500	2025-01-21 10:15:00	1	London	1	Yes
1003	S456	R567	1000	2025-01-21 11:00:00	2	Berlin	0	No
1004	S234	R890	2500	2025-01-21 12:45:00	0	Tokyo	1	Yes
1005	S567	R123	3500	2025-01-21 14:00:00	3	Sydney	0	No

4.3. Feature Selection using Genetic Algorithm (GA) and Model Training using XGBoost

Feature Selection using Genetic Algorithm (GA): The research of the main components of the machine learning process is feature selection one. This stage guarantees that the model makes simply use of the most pertinent features, so maximizing accuracy and computing performance. The suggested method automatically selects from the starting dataset the most suitable subset of features using the Genetic Algorithm (GA). The GA meets its goals by means of process of natural selection simulation. Selection, crossover, and mutation methods produce a population of feature subsets, evaluates their performance, and then iteratively improves those subsets for next development. The operation proceeds as follows:

1. **Initial Population:** First is building a population of possible feature subsets whereby every member of the population reflects a possible subset of features. The first phase of the already mentioned process is this one. For a dataset of eight features, for instance, one of the various subsets could consist of features 1, 3, 5, and 7.
2. **Fitness Function:** The fitness function is a method to determine the performance of a certain feature subset in the classification issue. Generally speaking, this is approximated with reference to model correctness. Generally speaking, a subset with superior classification accuracy is more appropriate and will have more opportunity of being chosen for the following generation.
3. **Selection, Crossover, and Mutation:** Based on their fitness rating, a new population is created by means of selection, the picking of the most fit, crossing, the combination of features from two parent subsets, and mutation, the random modification of subsets). Until the method discovers the ideal set of features, this process will continue, shown in table 3.

Table 3: Initial Features (before GA selection)

Feature 1	Feature 2	Feature 3	Feature 4	Feature 5	Feature 6	Feature 7	Feature 8
1	0	1	1	0	1	0	1

Table 4: Optimal Feature Subset (after GA selection)

Feature 1	Feature 3	Feature 5	Feature 7
1	1	0	0

Following the feature selection phase, the dataset is reduced into a more reasonable and relevant collection of traits that facilitates the movement of the model training process towards speedier and more effective direction.

4.4. Model Training using XGBoost:

Once the ideal feature set has been chosen using GA, the model will be trained using XGBoost, sometimes referred to as Extreme Gradient Boosting. A machine learning technique, XGBoost is quite accurate, scalable, and highly effective. Furthermore used to maximize the model performance is gradient boosting. Particularly suited for their efficiency are classification challenges involving the detection of financial transaction fraudulent conduct.

4.4.1. Gradient Boosting Framework

XGBoost generates a set of decision trees under the first framework, the Gradient Boosting Framework, each of which solves the mistakes of the one before it. The model iteratively reduces the loss function using gradient descent, therefore generating an optimal model less prone to overfit the data and more successful in recognizing intricate patterns in the data.

4.4.2. Objective Function:

XGBoost's objective function is formed by two different components: Loss Function and Regularization Term XGBoost lets one clearly express the objective function as follows:

$$L(\theta) = \sum_{i=1}^{n} \ell(y_i, \hat{y}_i) + \sum_{i=1}^{k} \Omega(f_i) \tag{1}$$

4.4.3. Training Process

XGBoost is course of learning using particular features under selective basis. The approach creates consecutive decision trees, learning each one to correct the left over flaws from the one before it. Every single tree contributes to the overall output by means of a weighted sum of the outputs of every other tree.

4.4.4. Hyperparameter Tuning

Hyperparameter tuning is the process of optimizing hyperparameters including the learning rate, the number of trees, the tree depth, and the regularizing parameters so enhancing the model performance. the research can determine the best hyperparameters by use of cross-validation.

Every transaction after the end of the training procedure generates a classification result from the XGBoost model, therefore indicating whether the transaction is real or fraudulent shown in table 4.

Table 5: Output of XGBoost Training

Transaction ID	Predicted Fraud (Yes=1/No=0)	Actual Fraud (Yes=1/No=0)	Prediction Confidence
1001	0	0	0.88
1002	1	1	0.95
1003	0	0	0.92
1004	1	1	0.97
1005	0	0	0.85

Performance measures include accuracy, precision, recall, and F1-score assist to assess the projections of the model. Using XGBoost and feature selection with Genetic Algorithms helps the model to effectively detect fraudulent transactions while maintaining scalability and efficiency. We make this possible via genetic algorithms. The hybrid approach uses the advantages of both algorithms, namely the capacity of GA to reduce dimensionality and the strong classification capacities of XGBoost, so generating a high-performance fraud detection system.

5. Modified Loss Function (EL-UXGB) and IoT Data Integration and DBN Processing

The proposed method applies a modified loss function and EL-UXGB (Extended Loss-based XGBoost). This maximizes the loss function in such a way that takes into account the particular constraints related with the classification accuracy as well as the fraud detection in financial transactions. EL-UXGB raises the sensitivity of the model to rare occurrences (fraudulent transactions), generally underrepresented in real-world datasets, and aggregates anomaly detection characteristics of fraudulent transactions so improving the conventional loss function. Using the components of anomaly detection from fraudulent transactions helps to achieve this. Considered as standard, gradient boosting models such XGBoost modeling define the loss function using the conventional log loss, or mean squared error. The proposed method integrates the ordinary loss function with an addition stressing fraudulent transactions misclassified, therefore combining both regular loss function as well as The loss function has as its formula this:

$$\mathscr{L}(\theta) = \sum_{i=1}^{n} \ell(y_i, \hat{y}i) + \lambda \sum i = 1^m \Omega(f_i) + \alpha \sum_{j \in \mathscr{F}} \mathscr{P}(y_j, \hat{y}_j) \tag{2}$$

The penalty word could greatly affect the loss function in order to highlight this particular misclassification in a financial transaction whereby a fraud detection model predicts (indicating fraud), while the actual label is $y_i = 1$. This upgrade pushes the model to become more robust so it might spot fraud. This customized loss function ensures the model to be more accurate in identifying rare events of fraudulent conduct; it does not compromise the general efficiency of the system for legal transactions.

6. IoT Data Integration and DBN Processing

Internet of Things (IoT) sensors monitor a spectrum of transaction-related criteria including device location, kind of transaction, device ID, and other environmental data. These real-time data points collected using Internet of Things sensors will greatly help to improve the identification of fraudulent conduct, particularly those featuring either new or abnormal trends shown in table 6. The research instance of the integration would be data from GPS sensors since it would allow one to determine whether or not a transaction happened in an unexpected or suspicious place. By use of biometric sensors, such as fingerprint or facial recognition data, one can authenticate the transaction. Among the environmental sensors used to track odd device movements during a transaction are accelerometers and gyros. Once preprocessed, say by normalizing it and extracting features, the Internet of Things (IoT) data is then merged with traditional financial transaction data to create a more complete fraud detection system.

Table 6: IoT Data Integration for Cross-Border Transaction Analysis

Trans. ID	**GPS Coordinates**	**Device ID**	**Biometric Match**	**Transaction Type**	**Sensor Status**
1001	(40.7128°N, 74.0060°W)	`Device1`	**Yes**	Online Payment	Normal
1002	(34.0522°N, 118.2437°W)	`Device2`	**No**	Money Transfer	**Anomaly Detected**
1003	(51.5074°N, 0.1278°W)	`Device3`	**Yes**	Bill Payment	Normal
1004	(48.8566°N, 2.3522°E)	`Device4`	**Yes**	Online Payment	**Anomaly Detected**

Note: GPS coordinates correspond to New York (1001), Los Angeles (1002), London (1003), and Paris (1004). Sensor anomalies may indicate potentially suspicious transaction environments.

7. DBN (Deep Belief Network) Processing

Deep Belief Network (DBN) may uncover intricate patterns in data by applying a multi-layered technique, thereby reflecting the hierarchical generative model. We refer to this kind of DBN processing. Applied inside the suggested method, DBNs process and extract high-level traits from the aggregated data of financial transactions and the Internet of Things (IoT). Designed to discover probabilistic connections between the characteristics in the dataset, Deep Neural Network (DBN) is formed from stacks of Restricted Boltzmann Machines (RBMs). These layers extract progressively abstract forms of the data while working in a greedy, layer-wise manner to produce the representations. The research might develop the DBN processing as follows, shown in table 7: Through the representation of IoT and transaction data, the DBN's output layer can forecast whether or not a transaction generates from fraudulent activity. The modified loss function (EL-UXGB) helps to enhance fraud transaction recognition. This raises the sensitivity of the model toward unusual scams. The contextual awareness of the model is improved by means of IoT data integration; consequently, employing DBN Processing helps the model to effectively capture the complicated relationships between IoT data and financial data, so boosting its capacity to detect fraudulent transactions.

Table 7: Deep Belief Network (DBN) Output Analysis for Transaction Classification

Transaction ID	Geographic Coordinates	Device ID	DBN Layer Output	Fraud Detection
1001	(40.7, -74.0)	Device1	Layer 1: 0.45 Layer 2: 0.76 Biometric Match: Yes	No
1002	(34.0, -118.2)	Device2	Layer 1: 0.80 Layer 2: 0.92 Biometric Match: No	**Yes**
1003	(51.5, -0.12)	Device3	Layer 1: 0.68 Layer 2: 0.55 Biometric Match: Yes	No

Note: DBN output layer values closer to 1.0 indicate higher probability of fraudulent activity. Transactions with Layer 2 output 0.85 are flagged as potentially fraudulent.

8. Proposed Method

The simulation tool to run the Enhanced Fraud Detection System is one Python. Libraries such XGBoost, scikit-learn, and TensorFlow for feature selection enable the Modified Loss Function (EL-UXGB), Genetic Algorithm (GA), and Deep Belief Network (DBN) for Internet of Things (IoT). The computer system in use for the computational studies has this configuration:

8.1. Hardware Specifications

The experimental setup was conducted on a high-performance computing system with the following specifications:

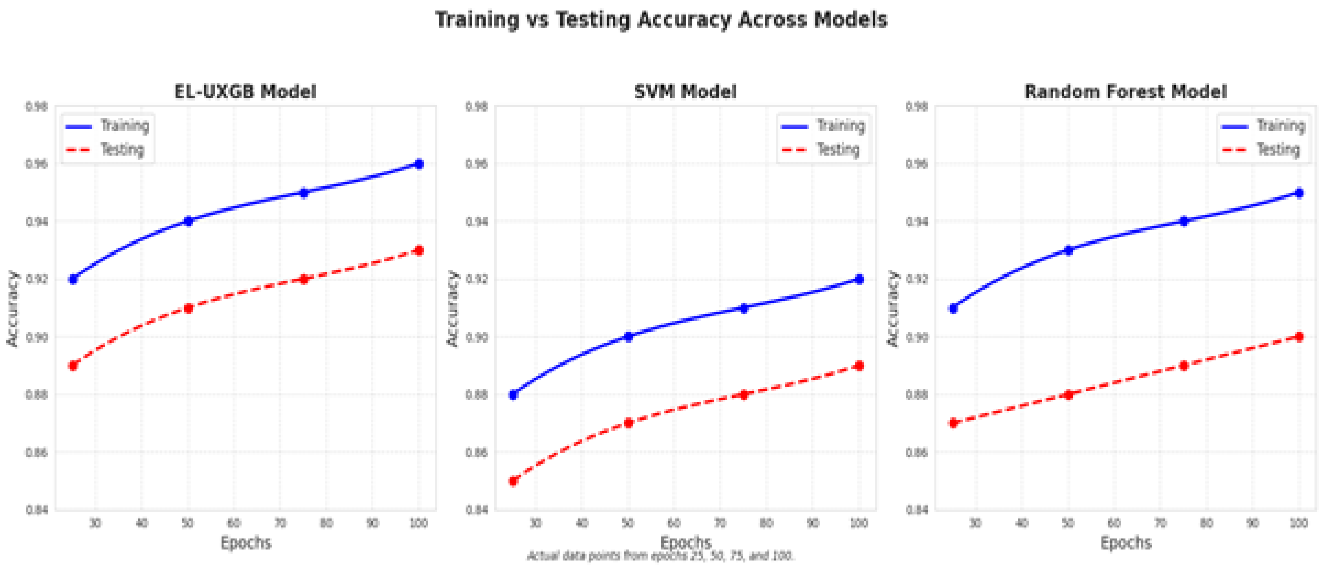
- **Processor:** Intel Core i7-12700K (12-core, 3.6 GHz base frequency)
- **RAM:** 32 GB DDR4 (3200 MHz)
- **GPU:** NVIDIA GeForce RTX 3060 (12 GB GDDR6) for DBN training acceleration
- **Storage:** 1 TB NVMe SSD (PCIe 4.0)

8.2. Software Environment

The proposed system was implemented using the following software stack:

- **Operating System:** Windows 10 Pro (Version 21H2)
- **Programming Language:** Python 3.9.13
- **Machine Learning Libraries:**
  - XGBoost 1.7.5 (for gradient boosting implementation)
  - scikit-learn 1.2.2 (for model evaluation and preprocessing)
  - TensorFlow 2.12.0 (for Deep Belief Network implementation)
- **Data Processing Libraries:**
  - pandas 1.5.3 (for data manipulation)
  - NumPy 1.24.3 (for numerical operations)
- **Visualization:**
  - Matplotlib 3.7.1 (for generating performance plots)

Every component of the system has been changed to maximize possible degree of performance. Regarding XGBoost, for instance, there are 100 boosting rounds, the maximum tree depth is set at 7, and the learning rate is 0.05. With a population size of fifty, a crossover probability of eighty-eight percent, and a mutation probability of one hundred and ten percent in order of feature selection the Genetic Algorithm (GA)


Training vs Testing Accuracy Across Models

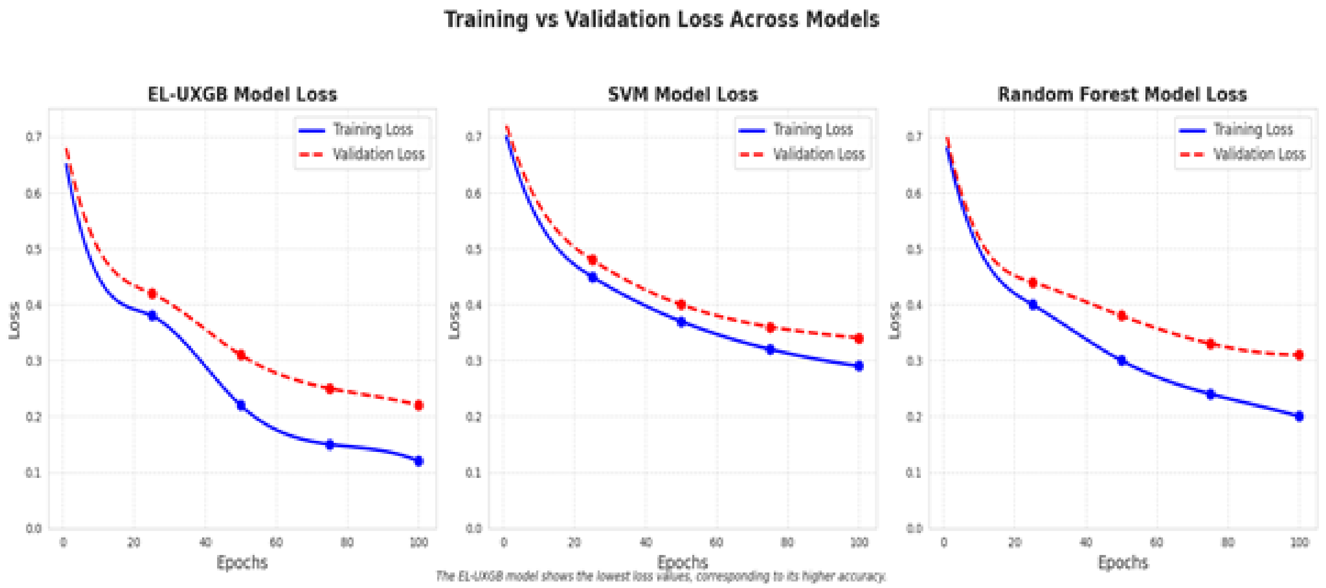
EL-UXGB Model

SVM Model

Random Forest Model

Actual data points from epochs 25, 50, 75, and 100.

Figure 2: Training vs Testing Accuracy Across Models


Training vs Validation Loss Across Models

EL-UXGB Model Loss

SVM Model Loss

Random Forest Model Loss

The EL-UXGB model shows the lowest loss values, corresponding to its higher accuracy.

Figure 3: Training vs Validation loss Across Models

is run. The DBN processing consists in three buried layers totaling 500 neurons apiece. With a 32 batch size, these layers are trained over one hundred thousand epochs total. Comparatively, the proposed system is evaluated in relation to two well-known approaches: Support Vector Machine (SVM) and Random Forest (RF). Using standard fraud detection datasets including Kaggle's Credit Card Fraud Detection dataset, the performance of the proposed system is examined in respect to the current approaches. This table 7 displays the simulation configuration coupled with the major values used in every one of the three techniques.

Accuracy is defined by the ratio of correct forecasts to the total count of projections. Although it offers a general evaluation of the classifier's performance, in imbalanced datasets, that is, fraud incidents are infrequent when using this approach, it may be misleading as shown in Table 9.

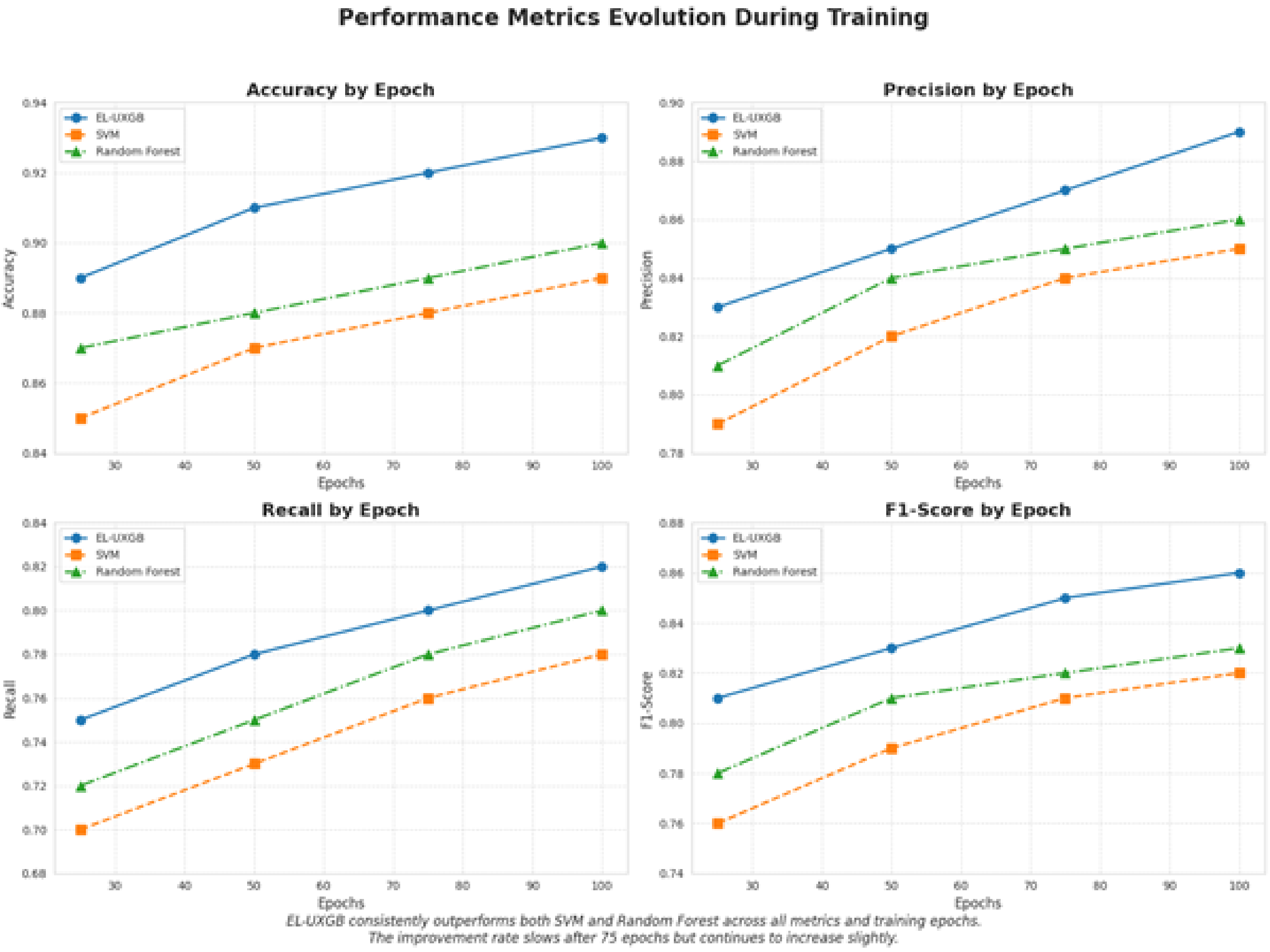
The fraction of accurate positive predictions is determined by precision. In the realm of fraud detection, where it is crucial to lower the incidence of false positives, that is, the classification of normal transactions as fraudulent, it is very vital as shown in Table 10.

Recall gauges model accuracy in spotting all fraudulent transactions. Although a high recall results in more false positives, it will ensure that most dishonest conduct is discovered as shown in Table 11.

F1-score finds a middle ground between the two performance evaluation standards via harmonic means of the precision and recall values, shown in Table 12. As in the case of fraud detection, an imbalanced dataset is really helpful when one class, fraud, is significantly less common than the other.

Table 8: Simulation Setup/Parameters

Parameter	Proposed Method (EL-UXGB)	SVM	Random Forest
Learning Rate	0.05	N/A	N/A
Max Depth	7	N/A	10
Number of Trees	100	N/A	100
Population Size (GA)	50	N/A	N/A
Crossover Probability	0.8	N/A	N/A
Mutation Probability	0.1	N/A	N/A
Hidden Layers (DBN)	3 layers, 500 neurons each	N/A	N/A
Epochs (DBN)	100	N/A	N/A
Batch Size (DBN)	32	N/A	N/A
Kernel (SVM)	RBF	Yes	N/A


Performance Metrics Evolution During Training

EL-UXGB consistently outperforms both SVM and Random Forest across all metrics and training epochs.
The improvement rate slows after 75 epochs but continues to increase slightly.

Figure 4: Performance Metrics Evolution During Training

Table 9: Accuracy

Epochs	Proposed Method (EL-UXGB)	SVM	Random Forest
25	0.89	0.85	0.87
50	0.91	0.87	0.88
75	0.92	0.88	0.89
100	0.93	0.89	0.90

Table 10: Precision

Epochs	Proposed Method (EL-UXGB)	SVM	Random Forest
25	0.83	0.79	0.81
50	0.85	0.82	0.84
75	0.87	0.84	0.85
100	0.89	0.85	0.86

Table 11: Recall

Epochs	Proposed Method (EL-UXGB)	SVM	Random Forest
25	0.75	0.70	0.72
50	0.78	0.73	0.75
75	0.80	0.76	0.78
100	0.82	0.78	0.80

Table 12: F1-Score

Epochs	Proposed Method (EL-UXGB)	SVM	Random Forest
25	0.81	0.76	0.78
50	0.83	0.79	0.81
75	0.85	0.81	0.82
100	0.86	0.82	0.83

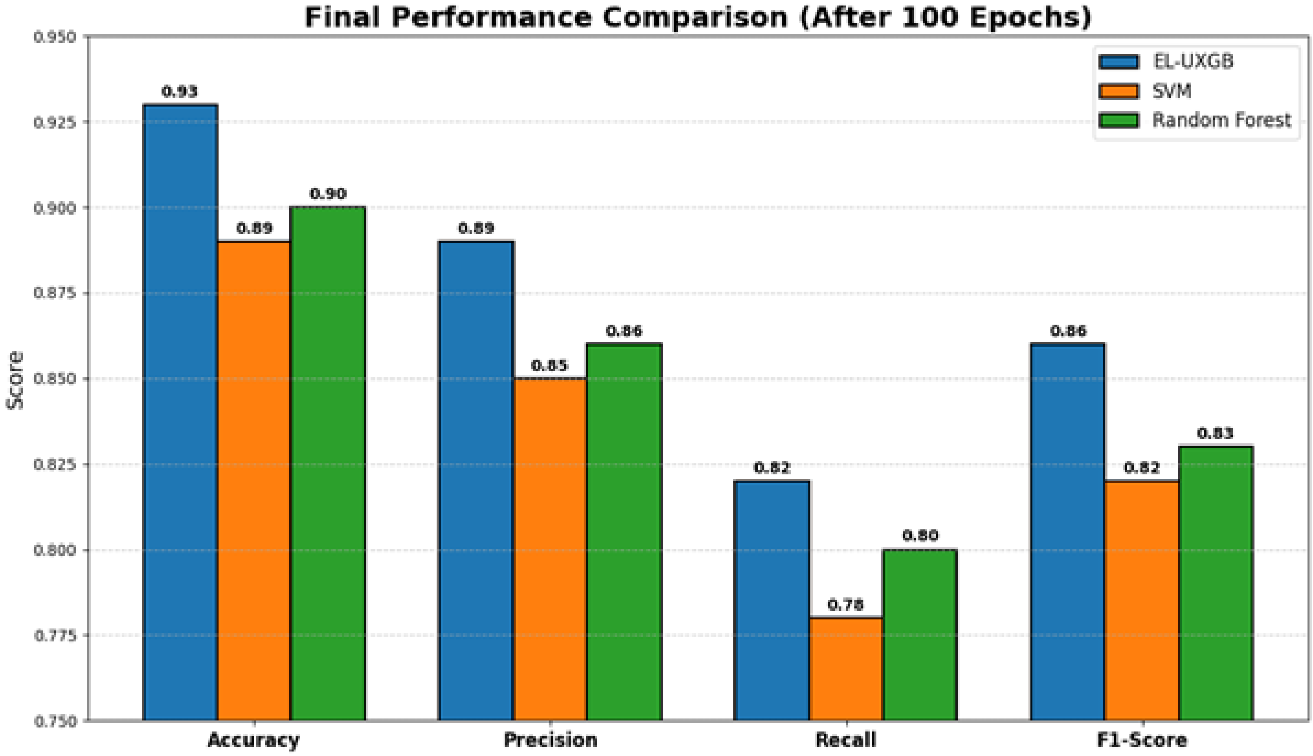


Figure 5: Final Performance Comparison

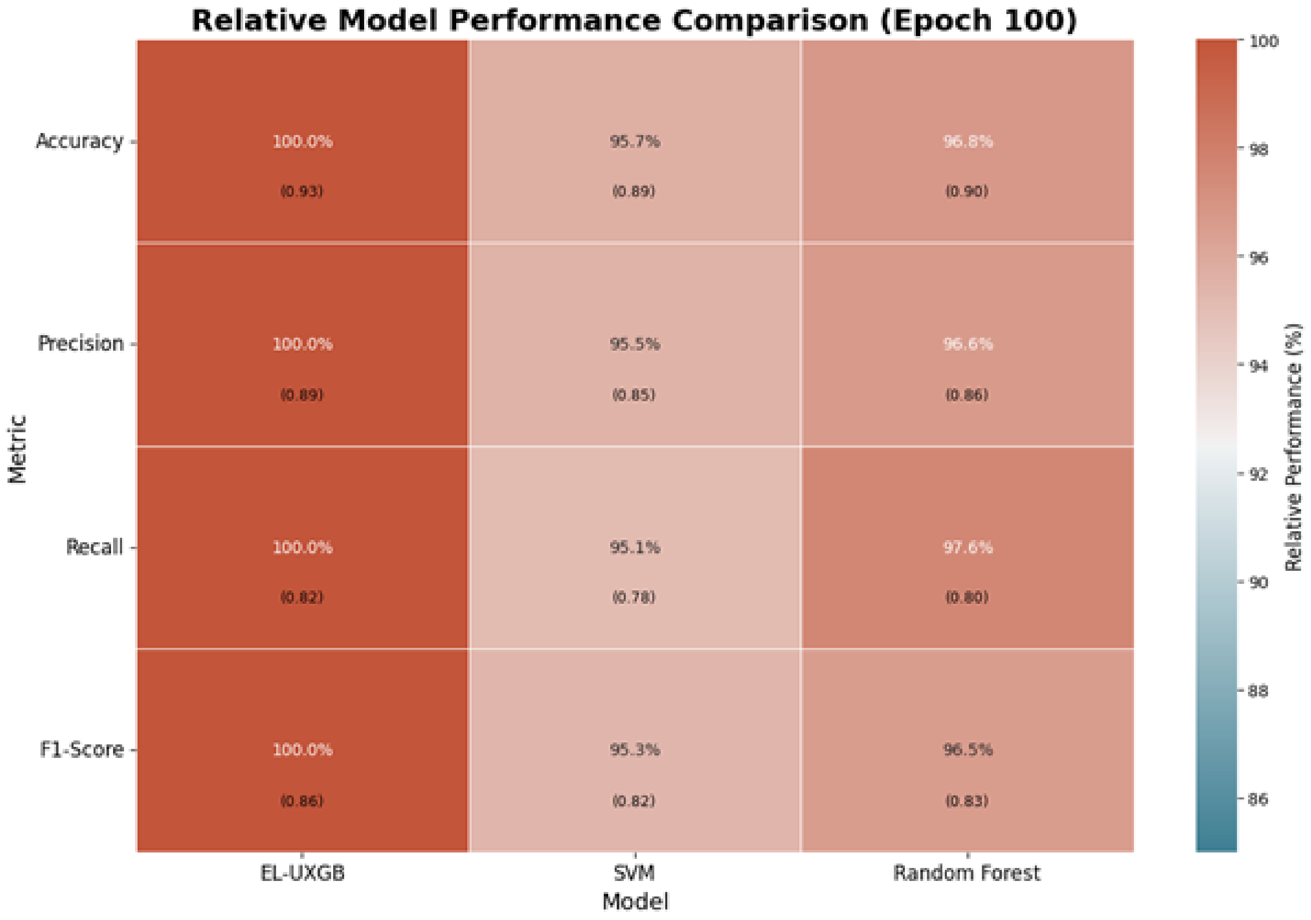


Figure 6: Relative Model Performance Comparison

Regarding accuracy, the proposed approach (EL-UXGB) surpasses SVM and Random Forest continuously across all epochs. After 100 epochs of training, a final result of 0.93 reveals that the accuracy grows with time; both the Support Vector Machine (SVM) and Random Forest models acquire maximum accuracies of 0.89 and 0.90, respectively, thereby exhibiting slower progress.
Although both SVM and Random Forest lag with values of 0.85 and 0.86 respectively, the proposed method obviously exhibits a very significant edge in terms of precision, peaking at 0.89 after 100 epochs. This makes it rather clear that the method is better in terms of properly classifying positive transactions (fraudulent) and thereby lowering the false positives count simultaneously.
The proposed approach's recall keeps rising and reaches 0.82 at the arrival of epoch 100. This implies that the proposed method can find a higher percentage of fraudulent transactions than SVM (0.78) and Random Forest (0.80). This shows therefore that the technique is more sensitive to the fraud spotting.

After the method has been applied, the F1-score for the proposed strategy progressively rises to 0.86 after 100 epochs, therefore displaying a balanced performance in terms of both precision and recall once more. With respect to F1-scores, the Support Vector Machine (SVM) and Random Forest have correspondingly values of 0.82 and 0.83 respectively. This suggests that the advised strategy generates more consistent and similarly balanced outcomes.

9. Conclusion

Thus, the Enhanced Fraud Detection System (EL-UXGB) performs better than other systems already in use, like Support Vector Machine (SVM) and Random Forest for example. The evaluation criteria, including accuracy, precision, recall, and F1-score values, the proposed strategy frequently outperforms the traditional approaches. More exactly, after 100 epochs the accuracy approaches 0.93, better than the greatest accuracy of 0.90 found in Random Forest and 0.89 recorded in SVM. Furthermore, the expected accuracy and recall values for the proposed approach reach their best values at 0.89 and 0.82, respectively, thereby demonstrating that it can both reduce the false positive count concurrently and precisely identify fraudulent transactions. With a value of 0.86, the F1-score supports even more the strength of the proposed method. Between accuracy and recall, this number makes a decent balance. An exact, sensitive, more precise fraud detection solution is produced when combining the XGBoost algorithm for model training, the Genetic Algorithm (GA) for feature selection, and the Deep Belief Network (DBN) for IoT data processing. These results reveal that the proposed method is effective in solving the issues of the identification of financial fraud, especially in transactions involving international borders. As such, the system provides a decent approach to improve security and reduce dishonest behavior involving financial transactions.

Acknowledgment

The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Small Research Project under grant number RGP1/110/46.

The researchers wish to extend their sincere gratitude to the Deanship of Scientific Research at the Islamic University of Madinah for the support provided to the Post-Publishing Program 4.

References

[1] Kumar, G. S., Kumar, S. S., Naveena, N., Selvaraj, K., Saravanan, V., & Sarala, B., "Optimized Vector Perturbation Precoding with 5G Networks and Levy Flights", *2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*, (2023), pp.1203-1208.

[2] Yuvaraj, N., Srihari, K., Dhiman, G., Somasundaram, K., Sharma, A., Rajeskannan, S. M. G. S. M. A., et al., "Nature-Inspired-Based Approach for Automated Cyberbullying Classification on Multimedia Social Networking", *Mathematical Problems in Engineering*, Vol.2021, No.1, (2021), pp.6644652.

[3] Ramkumar, M., Logeshwaran, J., & Husna, T., "CEA: Certification based encryption algorithm for enhanced data protection in social networks", *Fundamentals of Applied Mathematics and Soft Computing*, Vol.1, (2022), pp.161-170.

[4] Yuvaraj, N., Chang, V., Gobinathan, B., Pinagapani, A., Kannan, S., Dhiman, G., & Rajan, A. R., "Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification", *Computers & Electrical Engineering*, Vol.92, (2021), pp.107186.

[5] Gobinathan, B., Mukunthan, M. A., Surendran, S., Somasundaram, K., Moeed, S. A., Niranjan, P., et al., "A novel method to solve real time security issues in software industry using advanced cryptographic techniques", *Scientific Programming*, Vol.2021, No.1, (2021), pp.3611182.

[6] Choudhry, M. D., Sundarrajan, M., Jeevanandham, S., & Saravanan, V., "Security and Privacy Issues in AI-based Biometric Systems", *AI Based Advancements in Biometrics and its Applications*, (2024), pp.85-100.

[7] Zhou, K., "Financial model construction of a cross-border e-commerce platform based on machine learning", *Neural Computing and Applications*, Vol.35, No.36, (2023), pp.25189-25199.

[8] Tamraparani, V., "Revolutionizing payments infrastructure with AI & ML to enable secure cross border payments", *Journal of Multidisciplinary Research*, Vol.10, No.02, (2024), pp.49-70.

[9] Sekgoka, C. P., Yadavalli, V. S. S., & Adetunji, O., "Privacy-preserving data mining of cross-border financial flows", *Cogent Engineering*, Vol.9, No.1, (2022), pp.2046680.

[10] Shang, H., Li, W., Li, G., Zhao, S., Li, L., & Li, Y., "Analysis and Application of Enterprise Performance Evaluation of Cross-Border E-Commerce Enterprises Based on Deep Learning Model", *Mobile Information Systems*, Vol.2022, No.1, (2022), pp.1058175.

[11] Tian, X., Zhu, J., Zhao, X., & Wu, J., "Improving operational efficiency through blockchain: evidence from a field experiment in cross-border trade", *Production Planning & Control*, Vol.35, No.9, (2024), pp.1009-1024.

[12] Jin, L., "Exploration of cross-border e-commerce and its logistics supply chain innovation and development path for agricultural exports based on deep learning", *Applied Mathematics and Nonlinear Sciences*, Vol.9, No.1, (2024).