University of Ibadan
Journal of Science and Logics in ICT Research

A Machine Learning-Based Fraud Prevention Model for Improving Customers' Trust in E-Commerce

[1]✉ Olutayo V. A., [2]Akinwonmi A. E., and [3]Adewale O. S

Department of Computer Science, Federal University of Technology, Akure, Nigeria
vaolutayo@futa.edu.ng; aeakinwonmi@futa.edu.ng; adewale@futa.edu.ng

Abstract

The growth of e-commerce has led to significant challenges regarding fraud, resulting in a decline in customer trust and confidence in online transactions. This research proposes a comprehensive Fraud Prevention Model aimed at enhancing customer trust and security within e-commerce platforms by integrating advanced machine learning (ML) techniques, an Address Verification System (AVS), and Two-Factor Authentication (2FA). The model leverages Convolutional Neural Network - Long Short-Term Memory Network (CNN-LSTM) and Random Forest techniques to capture the complexities and temporal dependencies of e-commerce transaction data. The AVS component of the system verifies transaction legitimacy by comparing billing addresses with credit card records, and the implementation of 2FA adds an extra layer of security. The system's effectiveness was evaluated through rigorous testing using a dataset of transaction records. The results indicate that the combined approach of machine learning, AVS, and 2FA significantly enhances the detection of fraudulent transactions and improves overall customer trust in e-commerce platforms.

Keywords: *Machine Learning, CNN-LSTM, Random Forest Classification, Fraud Detection, E-commerce Security.*

1. Introduction

E-commerce, short for electronic commerce, refers to the buying and selling of goods and services over the Internet. The concept of online shopping dates back to the 1970s, but it wasn't until the 1990s that it started gaining widespread popularity with the advent of the World Wide Web. Since then, e-commerce has witnessed exponential growth, transforming the way businesses operate and consumers shop. According to Statista, global e-commerce sales amounted to 4.28 trillion US dollars in 2020 and are projected to reach 6.38 trillion US dollars in 2024. This significant growth is attributed to factors such as the increasing penetration of smartphones and internet access, improved payment gateways, and the convenience offered to consumers in making purchases from the comfort of their homes (Statista 2021).

While e-commerce offers numerous advantages, it also introduces unique challenges, particularly concerning payment and transactional security. Online transactions involve the exchange of sensitive financial information, including credit card details, passwords, and personal data. As a result, e-commerce platforms have become attractive targets for fraudsters seeking financial gain or data theft, which has led to a decline in customer trust in performing online transactions[2]. Over the years, numerous high-profile security breaches have exposed the vulnerabilities of e-commerce websites. One such incident was the data breach of retail giant Target in 2013, where hackers gained access to 40 million credit and debit card accounts, resulting in an $18.5 million settlement for the company[13].

Overall, e-commerce continues to grow and evolve, driven by advancements in technology, changes in consumer behavior, and the increasing digitization of commerce worldwide[4]. It has become an integral part of the global economy, shaping how businesses and consumers engage in commerce.

Olutayo V. A. Akinwonmi A. E. and Adewale O. S (2025). A Machine Learning-Based Fraud Prevention Model for Improving Customers' Trust in E-Commerce. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR),* Vol. 13 No. 1, pp. 1 – 12.

Fraud prevention in e-commerce refers to the proactive measures taken by online businesses to identify, mitigate, and deter fraudulent activities aimed at exploiting vulnerabilities in the online transaction process, thereby safeguarding the integrity of the e-commerce ecosystem. The emergence of credit cards in the mid-20th century, for example, led to the need for fraud prevention measures to address issues such as stolen cards, unauthorized transactions, and counterfeit fraud.

Financial institutions began implementing security features, such as signature verification, card expiration dates, and magnetic stripes, to mitigate fraud risks associated with credit card transactions. With the advent of the internet and e-commerce in the late 20th century, new forms of fraud emerged, including online payment fraud, identity theft, and phishing scams[5]. This prompted the development of specialized fraud prevention tools, technologies, and practices tailored to the unique challenges of the digital marketplace.

Customer trust in e-commerce can be defined as the confidence, assurance, and reliance that consumers have in the integrity, security, and reliability of an online business or platform. It influences their willingness to engage in online transactions and their perceptions of the overall quality of the e-commerce experience. Customer trust is a critical factor influencing purchasing decisions and long-term relationships between consumers and e-commerce companies. When using new technologies, including the web and e-commerce, trust is considered essential.

A commonly cited reason for consumers not purchasing from internet vendors is the lack of trust. Thus, there is a need to promote trust and confidence on the internet. For consumers, security and privacy issues are perceived as barriers to shopping online. They desire confidentiality of their identity and personal information, fearing exposure to online fraud. The potential risk in e-commerce is greater because of the anonymity, distance, and lack of physical interactions. Therefore, improving consumer trust in e-commerce requires continual advancements in fraud prevention techniques.

E-commerce has experienced explosive growth, with global e-retail sales reaching trillions of dollars yearly and continuing to rise steadily[1]. This growth can be attributed to the proliferation of internet-enabled devices, the widespread adoption of online payment systems, and the convenience and flexibility offered by online shopping platforms. The COVID-19 pandemic accelerated the shift towards e-commerce, as consumers turned to online channels for their shopping needs due to lockdowns and social distancing measures [6]. However, e-commerce poses significant risks and challenges, particularly the threat of fraud. These fraudulent activities result in financial losses for businesses and erode consumer trust and confidence in online shopping platforms.

The rapid growth of e-commerce has been accompanied by an increase in fraudulent activities and cybercrime, which have severely impacted customer trust and confidence in online transactions. This poses a significant challenge for both consumers and businesses engaged in e-commerce. As technology advances, so too do the methods used by cybercriminals to perpetrate fraud, making it crucial for businesses to continuously improve their fraud detection and prevention strategies [7]. Without addressing these escalating threats head-on, the long-term stability and sustainability of online commerce are at risk. Protecting consumers, preserving business reputations, and fostering consumer confidence are now more important than ever. To achieve this, businesses must remain vigilant and proactive in evolving their defenses against ever-changing fraudulent tactics.

The aim of this research is to design a model that enhances customer trust through fraud prevention in e-commerce. By achieving this aim, this project seeks to contribute to a safer and more trustworthy online shopping experience for consumers.

2. Related Works

The role of fraud prevention in enhancing customer trust in e-commerce has been a subject of extensive research. Smith et al. investigated the factors influencing trust in e-commerce transactions, focusing on online shoppers' perspectives. Their qualitative study utilized interviews and surveys to identify key determinants of trust, including website security, brand reputation, transaction transparency, and customer service responsiveness[8]. While the study provided valuable insights, it was critiqued for its limited sample size and lack of quantitative analysis, which might have strengthened the validation of its findings.

Jones and Wang explored the impact of fraud prevention measures on customer trust, aiming to determine whether robust fraud prevention strategies enhance consumer confidence[9]. Using survey data from online consumers, the study highlighted that techniques such as two.-factor authentication (2FA) and transaction monitoring significantly improved trust. However, the study faced critiques regarding potential response biases inherent in survey methodologies and the subjectivity involved in assessing trust.

Gupta et al. proposed a machine learning-based fraud detection model tailored for e-commerce platforms [10]. Their methodology involved analyzing historical transaction data to develop algorithms capable of identifying fraudulent activities. The study demonstrated the effectiveness of machine learning in reducing fraud-related losses but was critiqued for the absence of real-world implementation and scalability testing, raising concerns about its practical applicability.

Incorporating insights from these studies, this research adopts a comprehensive approach to enhancing customer trust in e-commerce through fraud prevention mechanisms. Advanced security features, as identified by Smith et al., are integrated to address website security and transaction transparency concerns [8]. Additionally, the layered fraud prevention framework combines 2FA and transaction monitoring, aligning with Jones and Wang's findings [9].

Finally, leveraging the methodologies from Gupta et al[10], this study incorporates machine learning models to analyze address verification data, identify fraud patterns and adapt to emerging threats. These combined strategies aim to create a scalable, real-world applicable system that strengthens customer trust in e-commerce platforms.

3. Methodology

3.1 System Architecture

The system architecture provides a high-level design of the fraud detection system, integrating machine learning models, external payment services, and essential security features like Address Verification System (AVS) checks and two-factor authentication (2FA). This architecture is built to be both scalable and adaptable, ensuring that fraud detection remains effective across various e-commerce platforms, even as transaction volumes grow

The following are the key architectural components:

I. Data Layer

PostgreSQL is used for managing the database, which stores critical information like user data, transaction records, fraud detection logs, and AVS results. This layer supports the storage and retrieval of transaction details, which is essential for both real-time fraud detection and future analysis.

II. API Layer

The API layer, built using FastAPI, serves as the communication interface between the system, machine learning models, and external services. It is responsible for handling interactions related to detecting suspicious transactions, performing AVS checks, verifying 2FA, and managing payments through external services like PayPal.

III. Machine Learning Layer

This layer features two candidate machine learning models—CNN-LSTM and Random detect fraudulent transactions. The best-performing model, based on accuracy, will be selected for deployment in real-time fraud detection.

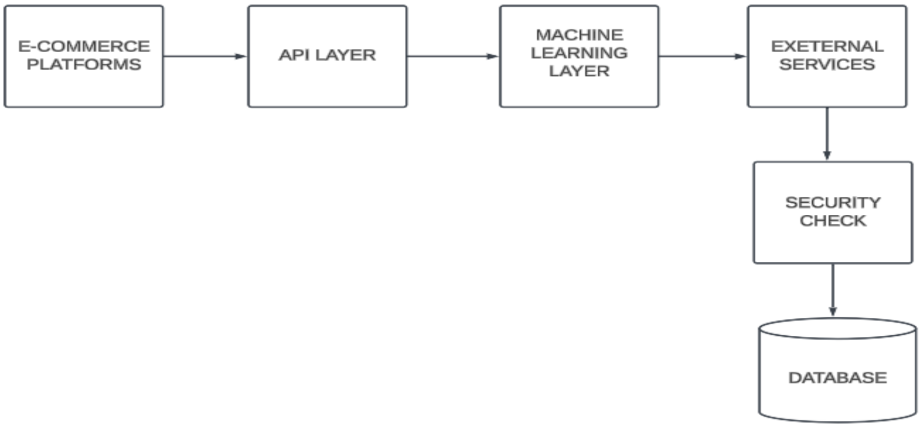


Figure 1: Proposed system architecture

IV. External Service Integration

PayPal's REST API is integrated to process payment transactions and conduct AVS checks. By comparing shipping and billing addresses, the system detects discrepancies that may indicate fraud. If such discrepancies are found, additional security measures, such as 2FA, are triggered to confirm the legitimacy of the transaction.

3.2 System Design

3.2.1 System Processes and API Workflow

This section outlines the fraud detection system's processes, from detecting suspicious transactions to final authorization with the role of each API endpoint.

I. Suspicious Transaction Detection

When a transaction is initiated, the system's API receives transaction details and evaluates them using the chosen machine learning model (CNN-LSTM or Random Forest). The model analyzed various features, such as transaction amount, order frequency, and transaction times, to classify the transaction as suspicious or legitimate. Suspicious transactions were forwarded to the next step.

II. *Security Questions*

If flagged as suspicious, the system prompted the user with security questions via an API. These questions validated the user's identity based on personal data. Correct answers allowed the process to continue, while incorrect answers blocked or flagged the transaction for further review.

III. Two-Factor Authentication (2FA)

After answering security questions correctly, the system initiated a 2FA process, sending a verification code to the user's registered mobile number or email. The user had to enter the code to proceed, adding an extra layer of security.

IV. Transaction Capture and AVS Check

Once 2FA was complete, the system captured the transaction details and performed an Address Verification System (AVS) check. An API request to the payment gateway (e.g., PayPal) checked if the billing and shipping addresses matched. Mismatches triggered further review or user confirmation.

V. Payment Authorization (via PayPal)

After successful verification, the payment authorization was processed through PayPal or another integrated payment gateway. If authorized, the user received a confirmation message, and the transaction was logged for future analysis. If denied, the user was notified, and the transaction was aborted.

3.2.2 System Development Tools

To develop the fraud prevention system, particularly the AVS framework for e-commerce, several design tools and technologies were employed for efficiency and robustness:

- **Python:** Python was used for machine learning model development. Python offered powerful libraries like TensorFlow and Scikit-learn. TensorFlow supported training complex models for real-time fraud detection, while Scikit-learn was used for implementing basic algorithms for initial testing and model development.
- **JavaScript:** Was employed for frontend development, ensuring an interactive user interface. JavaScript enhanced real-time interactions, which were essential for fast fraud detection and user feedback.
- **TensorFlow and Scikit-learn:** TensorFlow's scalability enabled large-scale model training, while Scikit-learn provided an efficient environment for implementing machine learning algorithms.
- **FastAPI:** FastAPI was used to build APIs for seamless integration between system components, ensuring smooth data exchange and interoperability with external platforms. RESTful APIs enhanced scalability and adaptability.
- **Zaron Cosmetics:** The case study for testing the AVS prototype was Zaron Cosmetics, a leading African cosmetic brand. With an established online presence and over 1,000 customer reviews, Zaron Cosmetics provided an ideal platform for evaluating the system's effectiveness in real-world e-commerce scenarios.

3.3 Data Collection and Analysis

The dataset used for training and testing includes both fraudulent and non-fraudulent transactions. Key features analyzed include:

- **Transaction Amount**: This feature captures patterns related to unusually large or small transactions that may suggest fraudulent activity.
- **Order Frequency**: Frequent small transactions or sudden spikes in order volume could signal potential fraud.
- **Location Mismatches**: Discrepancies between billing and shipping addresses are often a strong indicator of fraudulent behavior.
- **Unusual Transaction Times**: Transactions occurring at atypical times (e.g., late at night) might be flagged as suspicious.

To balance the dataset, synthetic data is generated by simulating normal and fraudulent activities. This helps to ensure a balanced dataset for training, with the generated synthetic transactions reflecting realistic deviations from baseline behaviors.

The final dataset consists of 25,000 records, with 40% fraudulent transactions and 60% legitimate ones. This distribution ensures that the machine learning models have enough examples of fraud to learn from while also mimicking real-world fraud rates.

3.4 Data Preprocessing

The preprocessing began with handling missing data, as incomplete entries can significantly impact model performance. To address this issue, techniques such as mean imputation for numerical data and mode imputation for categorical data were utilized. Formally, for a given feature X, the missing values Xi will be replaced by the mean μx, represented by the formula:

$$Xi = \frac{1}{n}\sum_{i=1}^{n} Xi$$

Data normalization was then applied to mitigate the effects of different scales among features (e.g., transaction amounts and frequencies). Min-max normalization was used to scale the data between 0 and 1, following the formula:

$$X' = \frac{X - X\min}{X\max - X\min}$$

Next, categorical variables such as payment methods and location details were converted into numerical representations using one-hot encoding. This approach transforms categorical data into a binary matrix, allowing each category to become a separate feature represented by values of 0 or 1.

Given the inherent imbalance in the real-world dataset, where non-fraudulent transactions significantly outnumber fraudulent ones, SMOTE (Synthetic Minority Over-sampling Technique) was employed to balance the dataset. This technique generates synthetic instances of the minority class (fraud) by interpolating between existing samples:

$$\begin{aligned} &\mathit{new\ sample} \\ &= \ \mathit{existing\ samplei} \\ &+ (\mathit{existing\ samplej} \\ &- \mathit{existing\ samplei}) \end{aligned}$$

Here, ʎ is a random number between 0 and 1, while existing sample$_i$ and existing sample$_j$ are two instances of the minority class.

3.5 *Feature Engineering and Selection*

Feature engineering focuses on selecting and creating features that help the model differentiate between fraudulent and non-fraudulent transactions. Important features include:

- **Transaction Amount**: The monetary value of each transaction, which may indicate spending patterns.
- **Order Frequency**: Analyzing how often a user makes purchases, can help detect anomalies such as sudden surges in activity.
- **Unusual Transaction Times**: Transactions occurring during unusual hours may raise flags for potential fraud.
- **Payment Methods**: Different payment methods may carry different levels of risk. This feature helps assess the likelihood of fraud based on how the transaction is processed.
- **Location Mismatches**: Discrepancies between the billing and shipping addresses identified by AVS checks, which can indicate potential fraud.

Recursive Feature Elimination (RFE) is used to select the most important features by removing those that contribute less to the model's predictive power. This helps improve model accuracy and reduce overfitting.

3.6 *Machine Learning Model Selection*

Two machine learning models, CNN-LSTM and Random Forest, are chosen for their ability to handle both sequential and static data patterns.

I. CNN-LSTM Model

This hybrid model combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. CNN captures spatial patterns, while LSTM models long-term dependencies in sequential data. This combination is particularly effective for identifying fraud patterns in transactional sequences.

Convolutional Layer

Extracts local features from the input data using filters (kernels), enhancing the model's ability to detect patterns. The output YYY from a convolutional layer can be calculated using the formula:

$$Y[i,j] = (X * K)[i,j] = \sum_{m}\sum_{n} X[m,n] \cdot K[i-m, j-n]$$

where:

X is the input data (e.g., a transaction matrix),

K is the kernel/filter,

(i,j) are the indices of the output feature map,

* denotes the convolution operation

LSTM Layer

The LSTM component is responsible for capturing long-term dependencies in sequential data. The LSTM updates its internal state using the following equations:

Forget gate f_t:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f$$

Input gate i_t:

$$i_t = \sigma(W_t \cdot [h_{t-1}, x_t] + b_i$$

Cell state $\hat{C}$:

$$\hat{C}_t = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c$$

Cell state update Ct:

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \hat{C}$$

Output gate o_t:

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o$$

Hidden state:

$$h_t = o_t \cdot \tanh(C_t)$$

Where:

W are weight matrices
b are bias vectors
Σ is the sigmoid activation function

Output Layer

The final output of the model is passed through a dense layer with a sigmoid activation function for binary classification (fraud or non-fraud).

II. Random Forest Model

This ensemble learning method builds multiple decision trees and combines their outputs to improve prediction accuracy. It is effective for analyzing independent features, such as transaction amounts and payment methods, which are critical for fraud detection.

Decision Tree Algorithm
At each decision point, the tree splits the data based on feature thresholds that maximize information gain, which can be measured using metrics like Gini impurity or entropy.
Random Forest Construction

The algorithm builds multiple trees on bootstrapped samples of the data, considering a random subset of features at each split to ensure diversity.

i.

ii. *Final Prediction*

iii. The model uses majority voting from individual trees to make the final classification decision (fraud or non-fraud).
Both models are trained independently and compared based on their performance metrics (accuracy, precision, recall, etc.). The best-performing model will be selected for deployment.

3.7 Model Training and Evaluation

Once the data was preprocessed, the machine learning models were trained on both real-world and synthetic datasets. To address the class imbalance between fraudulent and non-fraudulent transactions, SMOTE was applied, generating synthetic samples to balance the dataset and improve model training.

The models were evaluated using several performance metrics:

- **Accuracy (A)**: The ratio of correctly predicted transactions (both fraud and non-fraud) to the total number of transactions.

$$A = \frac{TP + TN}{TP + TN + FP + FN}$$

- **Precision (P)**: The proportion of transactions predicted as fraudulent that were indeed fraudulent.

$$P = \frac{TP}{TP + FP}$$

- **Recall (R)**: The proportion of actual fraudulent transactions correctly identified by the model.

$$R = \frac{TP}{TP + FN}$$

- **F1-Score (F1)**: The harmonic mean of precision and recall, offering a single performance measure.

$$F_1 = 2 \times \frac{P \times R}{P + R}$$

ROC-AUC Curve: The Receiver Operating Characteristic (ROC) curve was used to assess the model's ability to distinguish between fraudulent and non-fraudulent transactions. The Area Under the Curve (AUC) provided an overall performance evaluation.

The best-performing model, based on these metrics, was selected for deployment in the fraud detection system.

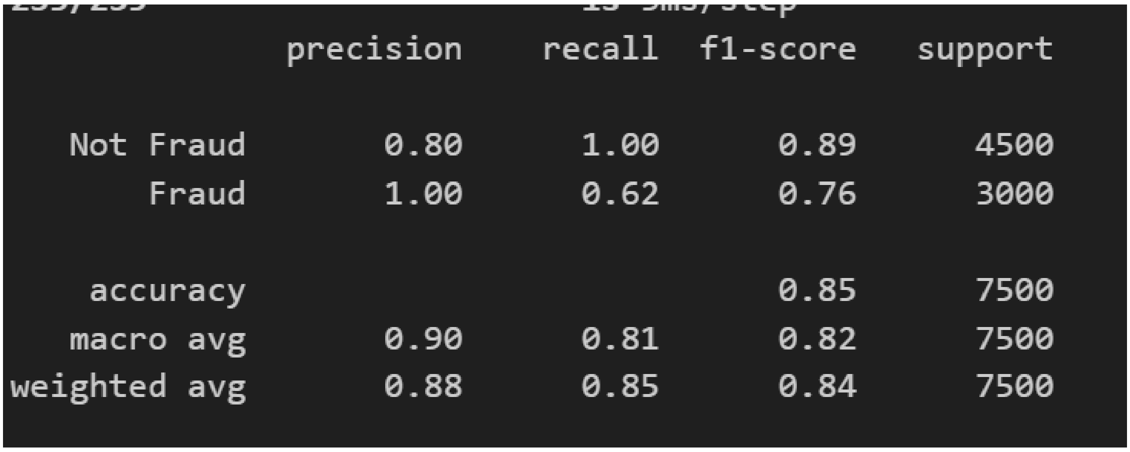
Once the data has been preprocessed, the machine learning models will be trained on both the real-world and synthetic datasets. To handle the class imbalance between fraudulent and non-fraudulent transactions, SMOTE will be applied to create a balanced dataset that enables the models to learn effectively.

The models will be evaluated using a variety of performance metrics, including:

4. Results and Discussion

4.1 Model Evaluation

The performance of the trained models was assessed using various classification metrics, which included accuracy, precision, recall, F1-score, and confusion matrix analysis. These metrics provided a comprehensive comparison between the CNN-LSTM and Random Forest models, offering insights into their effectiveness in fraud detection.

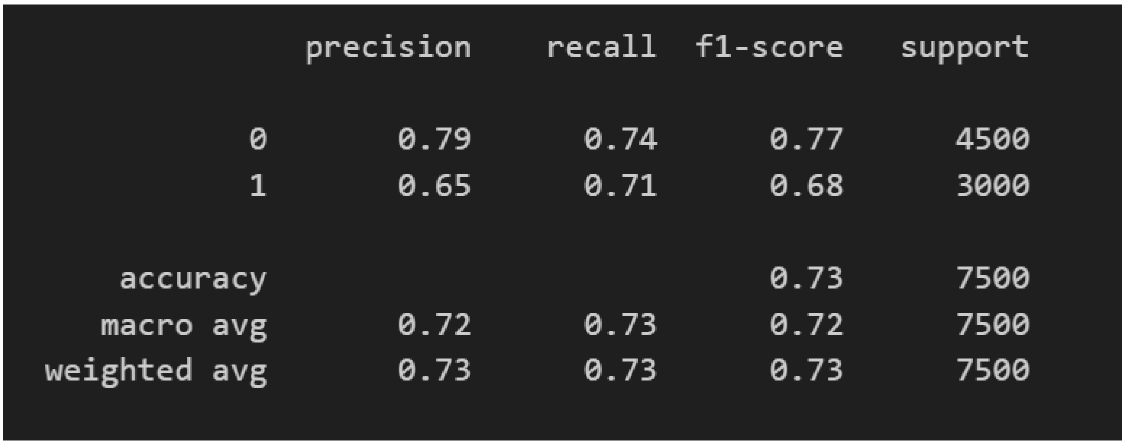


```
235/235                     1s 5ms/step
              precision    recall  f1-score   support

   Not Fraud       0.80      1.00      0.89      4500
       Fraud       1.00      0.62      0.76      3000

    accuracy                           0.85      7500
   macro avg       0.90      0.81      0.82      7500
weighted avg       0.88      0.85      0.84      7500
```

Figure 2: Classification report for CNN-LSTM model



```
              precision    recall  f1-score   support

           0       0.79      0.74      0.77      4500
           1       0.65      0.71      0.68      3000

    accuracy                           0.73      7500
   macro avg       0.72      0.73      0.72      7500
weighted avg       0.73      0.73      0.73      7500
```

Figure 3: Classification report for Random Forest Model

The classification report, summarized in Table 1, reveals that the CNN-LSTM model achieved higher overall performance compared to the Random Forest model. Specifically, the CNN-LSTM model demonstrated superior accuracy, precision, and recall, indicating its enhanced capability in correctly identifying fraudulent transactions. The F1-score, which balances precision and recall, also favored the CNN-LSTM model, highlighting its ability to minimize false positives and negatives more effectively.

Confusion matrix analysis was utilized to visualize the models' performance, showcasing the true positive, true negative, false positive, and false negative rates. This analysis revealed that the CNN-LSTM model was able to correctly classify a higher proportion of fraudulent transactions, thus affirming its robustness in a complex e-commerce environment.

Table 1: Comparison of Classification Metrics for CNN-LSTM and Random Forest Models

Metric	**CNN-LSTM**	**Random Forest**
Accuracy	0.85	I0.73
Precision	0.88	0.72
Recall	0.85	0.73
F1-Score	0.84	0.73

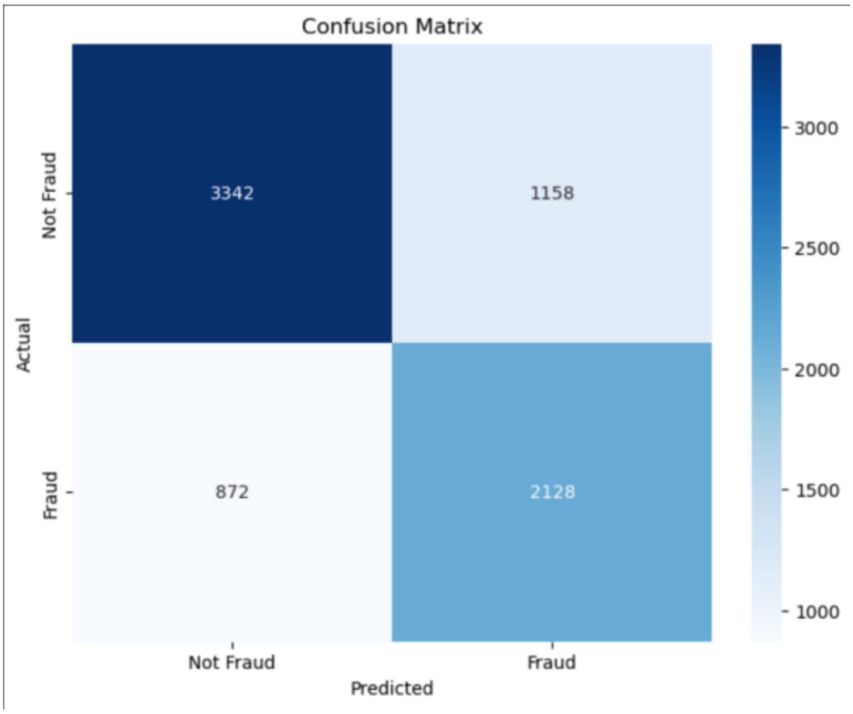


Figure 4: Confusion Matrix for random forest model

Overall, the evaluation results confirmed that the CNN-LSTM model not only outperformed the Random Forest model but also provided a more reliable solution for detecting fraudulent activities, thereby enhancing customer trust in e-commerce transactions.

The performance metrics were evaluated based on accuracy, precision, recall, F1-score, and confusion matrix analysis for both the CNN-LSTM and Random Forest models. The results demonstrated that the CNN-LSTM model outperformed the Random Forest model, achieving higher accuracy in detecting fraudulent transactions.

4.2 Discussion

The findings from the implementation of the Fraud Prevention Model reveal significant implications for enhancing customer trust and security in e-commerce transactions. The superior performance of the CNN-LSTM model over the Random Forest model highlights the effectiveness of deep learning techniques in capturing the complex patterns inherent in transactional data. This capability is crucial for accurately identifying fraudulent activities while minimizing false positives, which can deter legitimate customers.

Despite the promising results, several limitations were identified within the models and the overall system. For instance, the CNN-LSTM model, while more accurate, may require extensive computational resources and time for training, which could hinder its deployment in real-time scenarios[11]. Additionally, the effectiveness of the model is contingent on the quality and diversity of the training data. If the dataset does not adequately represent emerging fraud patterns, the model's performance may degrade over time.

Ongoing model training and validation using updated transaction data would help maintain the model's accuracy and adaptability to new fraudulent strategies[12]. This approach may involve implementing a feedback loop where the model learns from false positives and negatives, improving its predictions over time. Enhancing user experience is another critical area for improvement. The balance between security and convenience is vital; overly stringent security measures may lead to user frustration. Streamlining the security questions and 2FA processes could help create a smoother transaction experience, encouraging customer engagement while maintaining high security [13].

Furthermore, exploring additional security measures is essential to bolster customer trust further. Integrating biometric authentication, such as fingerprint or facial recognition, could provide an added layer of security that enhances user confidence. Additionally, implementing machine learning techniques for anomaly detection can provide real-time alerts for unusual transaction patterns, further safeguarding users[14].

In conclusion, while the Fraud Prevention Model has demonstrated effectiveness in reducing fraudulent transactions and increasing customer trust, addressing its limitations and continuously exploring enhancements will be essential for adapting to the evolving landscape of e-commerce fraud.

5. Conclusion

The implementation of the Fraud Prevention Model has proven to be a significant step forward in enhancing e-commerce security. The findings from this research highlight the transformative potential of analytics and machine learning in fraud prevention. With these tools, e-commerce businesses can better protect transactions and customer data, creating a more secure environment for online shopping.

To sustain and enhance the model's success, the following recommendations are proposed:

Continuous Model Improvement Regular updates and retraining of the CNN-LSTM model using fresh transactional data are crucial to maintaining its accuracy and adaptability. Fraudulent tactics evolve rapidly, and implementing a feedback loop to learn from false positives and false negatives will improve the model's predictive performance.

User Experience Optimization Security measures, while essential, must not compromise user convenience. Streamlining processes such as security questions and two-factor authentication (2FA) can enhance the customer experience, ensuring that security does not become a barrier to engagement or satisfaction.

Integration of Advanced Security Features Future iterations of the Fraud Prevention Model should incorporate cutting-edge security technologies, including biometric authentication (e.g., fingerprint or facial recognition). Additionally, integrating real-time anomaly detection algorithms can enable instant identification and mitigation of suspicious activities, making fraud prevention more proactive.

Comprehensive Training and Awareness Educating customers about the platform's security features and best practices for online safety is vital. Clear, accessible guidelines on using these features and identifying potential fraud will empower users to contribute to their security, enhancing overall trust in the platform.

Exploration of Alternative Models Expanding research into alternative machine learning and deep learning algorithms is recommended to optimize fraud detection. Techniques such as ensemble methods or hybrid approaches may offer improved accuracy, efficiency, and adaptability compared to CNN-LSTM and Random Forest models.

References

[1] Statista. (2024). *Retail e-commerce sales worldwide from 2014 to 2027 (in billion U.S. dollars)*. Retrieved December 8, 2024, from https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

[2] Jane, M., Samonte, C., Serrano, E., Anthony, J., Arpilleda, T., Leyton-Pete, R., Pastrana, J., Quijano, D., Robert, R., & Sulit, R. (2022). Implementing deep learning in e-commerce platforms for fraud detection and management. Proceedings of the International Conference on Industrial Engineering and Operations Management. https://doi.org/10.46254/an12.20220756

[3] Clay, K. (2013, December 18). *Millions of Target customers likely affected by data breach*. Forbes. Retrieved December 8, 2024, from https://www.forbes.com/sites/kellyclay/2013/12/18/millions-of-target-customers-likely-affected-by-data-breach/

[4] Deng, J. (2022). How customer behavior has transformed as e-commerce has developed in the digital economy. BCP Business & Management. https://doi.org/10.54691/bcpbm.v33i.2836

[5] Alam, F., & Ali, M. (2020). E-commerce benefits, challenges, and growth in India. International Journal of Computer Applications. https://doi.org/10.5120/ijca2020919920

[6] Guthrie, C., Fosso-Wamba, S., & Arnaud, J. (2021). Online consumer resilience during a pandemic: An exploratory study of e-commerce behavior before, during, and after a COVID-19 lockdown. Journal of Retailing and Consumer Services, 61, 102570. https://doi.org/10.1016/j.jretconser.2021.102570

[7] Altuk, E. (2021). Detection and prevention of fraud in the digital era. In Advances in Business Information Systems and Analytics (pp. 126–137). https://doi.org/10.4018/978-1-7998-4805-9.CH009

[8] Smith, A., et al. (2019). The Role of Trust in E-commerce Transactions. Journal of Consumer Research, 45(2), 217-235.

[9] Jones, B., & Wang, S. (2018). Impact of fraud prevention measures on customer trust. Journal of Marketing Research, 55(3), 342–359.

[10] Gupta, R., et al. (2020). Machine learning-based fraud detection in e-commerce. IEEE Transactions on Knowledge and Data Engineering, 32(5), 923–937.

[11] Hasugian, L., & Suharjito, S. (2023). Fraud detection for online interbank transactions using deep learning. Syntax Literate: Jurnal Ilmiah Indonesia. https://doi.org/10.36418/syntax-literate.v8i6.12627

[12] Ashfaq, T., Khalid, R., Yahaya, A., Aslam, S., Azar, A., Alsafari, S., & Hameed, I. (2022). A machine learning and blockchain-based efficient fraud detection mechanism. Sensors, 22(19), 7162. https://doi.org/10.3390/s22197162

[13] Kumar, K., & Gupta, H. (2021). Designing a security framework for enhancement of electronic transactions. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)
(ICRITO) (pp. 1–5). https://doi.org/10.1109/icrito51393.2021.9596545

[14] Li, Y., & Zhang, H. (2022). Fraudulent detection techniques in e-commerce: A systematic review. Computers in Human Behavior Reports, 8, 100260. https://doi.org/10.1016/j.chbr.2022.100260