Journal of Basics and Applied Sciences Research (JOBASR)
ISSN (print): 3026-9091, ISSN (online): 1597-9962
Volume 3(6) November 2025
DOI: https://dx.doi.org/10.4314/jobasr.v3i6.3

Toward Smart Financial Security: Design of Web-Based Credit Card Fraud Detection System

Barira Hamisu[1*], Raji Abdullahi Egigogo[2] & Ahamad Musa Bindawa[3]
[1,2&3]Department of Software Engineering and Cyber Security, Al-Qalam University, Katsina, Nigeria.
[*]Corresponding Author Email: barirahamisu@auk.edu.ng

ABSTRACT
As financial transactions become increasingly digital, there is an urgent need for stronger security measures. This paper presents a web-based credit card fraud detection system designed to address this challenge and enhance transaction security. The system was designed to provide an easy tool for identifying suspicious activity without relying on complex predictive models such as machine learning. It uses a Python backend linked to a SQLite database and a browser-based interface built with HTML, CSS, and JavaScript. The web-based credit card fraud detection system employs rule-based validation and anomaly checks that examine transaction amounts, frequency of use, and deviations from a cardholder's normal behavior. Evaluation involved unit, integration, performance, and security testing. The results suggest that the system performs well by identifying questionable transactions, maintaining stable operation under high transaction volumes, and resisted common security threats. While its rule-based design may limit adaptability to evolving fraud tactics, the system demonstrates that a straightforward web application can still offer meaningful protection for digital financial operations.

Keywords:
Credit Card Fraud,
Web-based system,
Fraud Detection.

INTRODUCTION

Credit Cards are rectangular pieces of plastic issued by banks to cardholders; they allow the cardholder to buy goods and services from merchants that accept card payments online or offline. The credit card is two-sided, its front-facing contains "the bank name, card number, card holder's name, the chip, and the expiry date", and its back "the magnetic strip, signature, hologram, and the Card Verification Code" (Onyema et al., 2023). Credit card transactions involve four include the consumer, the credit card issuer, the merchant, and the merchant's bank (Dhavapriya & Anuratha, 2024).

Credit cards offer a fast, convenient, and secure method for online and offline transactions, contributing to their global popularity (Chaudhary et al., 2012). However, the rise in credit card usage has led to increased fraud, with criminals continually exploiting financial system vulnerabilities (Singh, 2024). Users must remain cautious, as fraudsters illegally use card details to conduct unauthorized transactions, resulting in financial losses for both banks and individuals (Azeez et al., 2021).

There are mainly two types of purchases with credit cards online purchase and offline purchase. In online purchases or virtual purchases, the credit card is not present it is usually done online or by telephone. The customer provides information about the credit card expiry date, secure code, card number, etc. In contrast, in offline purchases the credit card has to be presented to make payment. Fraudsters abuse the two types of purchases, to commit online fraud, Fraudsters use the internet on either a computer or phone, to shop on the web in the absence of the card and make payment by providing some important information about the card. Most often the real card owner is not aware that a fraudster has stolen his/her card details and is not aware of the purchase. In offline fraud, the fraudster steals the card and forges the signature; if the cardholder does not recognize the loss, it leads to a financial loss (Chaudhary et al., 2012).

A fraudulent credit card transaction involves any unauthorized use of an individual's account by someone other than the legitimate owner, whether the transaction occurs online or offline. Such unauthorized activities can often be identified by analyzing the cardholder's historical purchasing behavior. People generally follow specific spending habits, and credit card users exhibit patterns regarding transaction locations, amounts, timings, and other details. A significant deviation from these usual patterns can indicate fraudulent activity (Onyema et al., 2023)

How to cite this article: Barira H., Raji A. E. & Ahamad M. B. (2025). Toward Smart Financial Security: Design of Web-Based Credit Card Fraud Detection System. *Journal of Basics and Applied Sciences Research*, *3*(6), 22-30. https://dx.doi.org/10.4314/jobasr.v3i6.3

Credit card fraud can take several forms, including application fraud, account takeovers, counterfeit cards, fraudulent merchant websites, and temporary accounts (Du et al., 2023; Jain, 2019).

The rapid expansion of online transactions has heightened the threat of credit card fraud, highlighting the urgent need for effective fraud detection systems. This study proposes the design and implementation of a web-based credit card fraud detection system aimed at delivering an efficient, scalable, and secure solution to identify fraudulent transactions.

Researchers have proposed several techniques in the literature to address the challenges associated with identifying fraudulent transactions using credit cards. Some of the fraud detection systems that have been developed in the literature include rule-based, statistical, and machine-learning techniques(Chatterjee et al., 2024; Hilal et al., 2022; Meduri, 2024; Kotagiri, 2023).

Rule-based fraud detection systems were among the first methods used to identify fraudulent activities. They operate using predefined rules, such as setting transaction amount limits, verifying location, and monitoring user behavior, based on expert insights and past fraud incidents. Although easy to implement and understand, these systems are limited in their ability to adapt to new and evolving fraud tactics, as fraudsters continually modify their strategies to bypass static rules (Chatterjee et al., 2024; Hilal et al., 2022). The rigidity of rule-based systems makes them slow to respond to emerging threats unless manually updated, a process that is labor-intensive and often falls behind the pace of fraud evolution (Meduri, 2024; Kotagiri 2023). Because the rules are broad enough to cover multiple fraud scenarios, they tend to generate a high number of false positives. Furthermore, since these systems rely on historical data and familiar fraud patterns, they are ineffective against novel or highly sophisticated frauds. Maintaining and scaling rule-based detection frameworks is resource-heavy and increasingly difficult as transaction volumes grow. Recently, a rule-based machine learning model has been introduced to improve financial fraud detection without the need for resampling, achieving a 98% accuracy rate and a 99% Matthews Correlation Coefficient (MCC) across two benchmark datasets. This modern approach combines transparency and interpretability, making it particularly valuable in the financial industry(Islam et al., 2024).

Statistical models play a vital role in fraud detection by applying mathematical and probabilistic methods to uncover anomalies and irregular transaction patterns. Through the analysis of historical transaction data, these models can detect inconsistencies and predict the likelihood of fraudulent behavior. As technology advances, detecting credit card fraud has become increasingly critical in financial operations. Various statistical methods have been introduced to address fraud challenges—such as combining data mining with statistical techniques like feature selection, resampling, and cost-sensitive learning, leading to a 14% reduction in misclassification costs (Beigi & Amin-Naseri, 2020). The Hidden Markov Model has also been proposed for identifying suspicious transactions (Dhok, 2012), while research emphasizes the importance of feature selection and data balancing to boost model effectiveness (Zou, 2024). These approaches aim to improve detection accuracy while minimizing false positives, potentially saving financial institutions billions each year (Gao et al., 2019; Ogundunmade & Adepoju, 2024).

Given the surge in online transactions and increasingly sophisticated fraud strategies, machine learning techniques have become essential for credit card fraud detection (Anjum et al., 2023; Zou, 2024) . Numerous models, including Neural Networks, Support Vector Machines (SVM), Decision Trees, Random Forests, K-Nearest Neighbors (KNN), and Logistic Regression, have been explored for their ability to detect fraud (Gao et al., 2019; Zou, 2024).

While Neural Networks and SVMs handle complex datasets effectively (Zou, 2024), a study indicates that Decision Trees offer the highest accuracy (Ogundunmade & Adepoju, 2024). Researchers have compared the performance of these classification algorithms and emphasized the challenges of imbalanced datasets, highlighting the importance of sampling strategies to enhance detection outcomes (Anjum et al., 2023; Chatterjee et al., 2024). Hybrid models that integrate multiple algorithms have also been explored for improved results, with findings often showing that Decision Trees outperform others across various evaluation metrics. Techniques like data mining (Chen et al., 1996), Supervised learning, Semi-supervised learning and Unsupervised learning (Bolton & Hand, 2002) (Zhu, 2008) have all been utilized to strengthen fraud detection efforts.

To overcome the limitations of single classifiers, recently studies have shifted toward ensemble and featured engineered models. A study by (Olaniran & Lawal, 2025)performed a comparative analysis which assed Random Forest, Gradient Boosting Machines and Stacking algorithms on a real-world transaction dataset enriched with temporal, behavioral, and geographic attributes. Their study found out that ensemble models always outperformed individual classifiers. Gradient Boosting Machines has the highest recall and balanced accuracy, this makes it suitable for detecting hidden fraud, while Stacking showed better precision and overall accuracy by reducing false positives. The result suggests that combining ensemble learning with targeted data preparation provides an effective foundation for building reliable fraud detection systems.

Several advances in the literature has been made, most of the existing literatures focus on algorithmic modeling rather than real-world system implementation. Many machine learning models are difficult, and computationally demanding for small financial institutions to deploy. This limitation encourages the interest in the design and implementation of a web-based detection system that rely on flexible, rule-based logic and secure web technologies to monitor transactions in real time. The systems emphasize accessibility, scalability, and ethical data handling, this shows effective fraud prevention can be achieved without relying on complex predictive models like machine learning. This study builds on this path by developing a practical web-based platform that applies rule-based and anomaly detection techniques within a secure, browser-accessible environment.

MATERIALS AND METHODS

The methodology adopted for this study focuses on the design, implementation, and evaluation of a web-based credit card fraud detection system. Requirement analysis, system design, rule creation, database structuring, implementation, and multi-level testing to confirm performance, security, and functionality were all steps in the process.

Software Methodology

Selecting an appropriate software development methodology is crucial for developing an effective Credit Card Fraud Detection System. The chosen methodology provides a structured approach to guide the study from inception through deployment and ongoing maintenance. The Agile methodology is selected for this study due to its flexibility and iterative approach, which is well-suited to adapt to evolving fraud patterns and regulatory changes.

Requirement Analysis

Requirement analysis is pivotal in developing a robust Credit Card Fraud Detection System. Key steps include identifying stakeholders, gathering specific fraud detection needs, analyzing existing fraud detection methods, documenting functional and non-functional requirements, creating use cases, validating requirements, prioritizing them, finalizing the requirement specification, and obtaining stakeholder approval.
Understanding stakeholders such as financial institutions, cardholders, and regulatory bodies is critical.

Data Description

A structured collection of transaction records, comprising transaction amount, time, merchant information, and user profile parameters, is used by the system's backend. Testing was conducted using a sample dataset of credit card transactions that had been anonymized. To guarantee accuracy in detection procedures, preprocessing involved data format validation, transaction value normalization, and inconsistent entry elimination. To protect privacy, sensitive data was anonymized prior to testing.

Mathematical Concept of the Web Based Credit Car d Detection

This section presents the mathematical formulation that governs the detection logic implemented within the web-based fraud detection system. The model operates as part of the server-side algorithm that automatically evaluates each incoming transaction and determines whether it should be approved or flagged as suspicious.
Each transaction request arriving at the system is represented as a feature vector:

$$\mathbf{x}_t = [x_{t,1}, x_{t,2}, \dots, x_{t,d}]^T \quad (1)$$

where each $x_{t,i}$ represents a transaction attribute such as amount, time, location, merchant ID, or device identifier. The system uses predefined rules and deviation thresholds stored in the database to compute a fraud risk score in real time.

Rule-Based Transaction Assessment

For every transaction x_t, the system compares selected attributes against threshold limits established during system configuration. For example:

$$r_{t,i} = \begin{cases} 1, & \text{if } |x_{t,i} - \mu_i| > \delta_i \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

where:

μ_i is the normal or historical average for attribute i,
δ_i is the acceptable deviation range,
$r_{t,i} = 1$ indicates a rule violation.

The overall rule activation score for the transaction is then computed as

$$R_t = \frac{1}{n}\sum_{i=1}^{n} r_{t,i} \quad (3)$$

Transaction Risk Scoring Function

The web system assigns a risk score S_t to each transaction by combining rule violations and attribute deviations:

$$S_t = \sum_{i=1}^{n} w_i \cdot f_i(x_{t,i}) \quad (4)$$

where:

w_i is the assigned importance weight for each attribute,
$f_i(x_{t,i})$ is a normalized function that returns higher values for abnormal attributes,
S_t represents the overall suspiciousness score.

If S_t exceeds a specified threshold τ, the transaction is automatically flagged by the backend logic as potentially fraudulent and forwarded to the administrator's dashboard.

$$\text{Transaction status} = \begin{cases} \text{Legitimate}, & \text{if } S_t \leq \tau \\ \text{Suspicious}, & \text{if } S_t > \tau \end{cases} \quad (5)$$

Web System Decision Flow

1. Input Stage: Transaction data is submitted through the web interface.
2. Computation Stage: The backend algorithm computes deviations and the total risk score S_t.
3. Decision Stage: Based on S_t, the system either approves the transaction or flags it.
4. Storage Stage: Results (status, time, and flag reason) are stored in the transaction database.
5. Notification Stage: If a transaction is flagged, an alert is generated and displayed on the web dashboard.
   Mathematically, the backend process can be summarized as:

$$\hat{y}_t = \begin{cases} 0, & S_t \leq \tau \quad \text{(Normal)} \\ 1, & S_t > \tau \quad \text{(Flagged)} \end{cases} \quad (6)$$

Adaptive Threshold Updating

To accommodate changing transaction behavior over time, the web system updates the normal value μ_i dynamically using a moving average which is given as

$$\mu_i^{(\text{new})} = \alpha x_{t,i} + (1-\alpha)\mu_i^{(\text{old})} \quad (7)$$

where $0 < \alpha < 1$ is the adaptation rate controlling how fast the system learns new user patterns. This allows the web platform to adapt to evolving financial activity without manual recalibration. Table 1 shows the pseudocode of the web based fraud detection system.

Table 1: Pseudocode for Web-Based Fraud Detection

Pseudocode for Web-Based Fraud Detection
Input: Transaction data x_t = [x1, x2, …, xn] Output: Transaction Status ∈ {Legitimate, Suspicious}
Begin
Receive x_t from web form
Retrieve μ_i and δ_i for user from database

Initialize S_t ← 0
For each feature i in [1…, n] do
Compute deviation d_i ← |x_t[i] - μ_i|
If d_i > δ_i then
r_i ← 1
Else
r_i ← 0
end if

If S_t > τ then
Transaction Status ← "Suspicious"
Generate alert and store in fraud_log table
else
Transaction Status ← "Legitimate"
end if
6. Update μ_i ← α * x_t[i] + (1 - α) * μ_i
7. Display Transaction Status on web dashboard
End

Evaluation Approach

Evaluation was centered on system performance and quality rather than predicted accuracy because the system is entirely web-engineered. The assessment comprised:

i. Functional Testing: Verified that every system module and fraud detection rule operated as planned.
ii. Integration testing: Confirmed that the database, backend logic, and web interface all communicated with each other seamlessly.
iii. Performance testing: To gauge the system's scalability, throughput, and reaction time, high transaction volumes were simulated.

Ethical and Privacy Considerations

Security testing evaluated resistance to threats of data manipulation, SQL injection, and illegal access attempts. The system was created in accordance with privacy-preserving standards since financial data is sensitive. Role-based authentication was used to restrict access and anonymize test data. User-specific data was protected from unwanted access, and encryption was used to secure data transmission. By preserving confidentiality and preventing financial information from being misused, the technique guarantees adherence to ethical principles.

System Design

System design for this study involves creating specifications for input data, database design, input procedures, and outputs. It focuses on developing a robust architecture that supports transaction monitoring, fraud detection algorithms, integration with external data sources, and compliance with security standards. Figure 1 shows the system architecture.

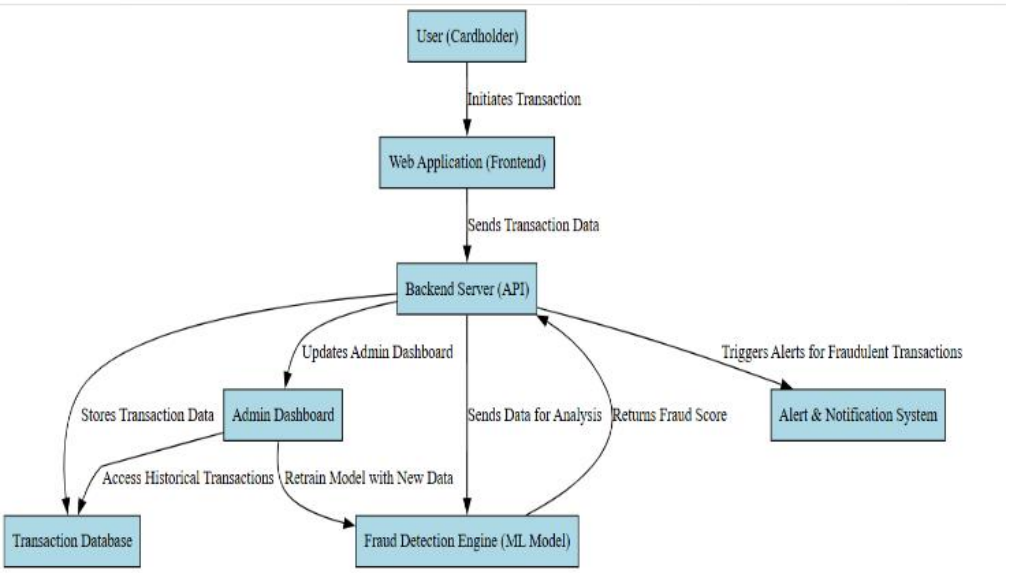

Figure 1: System architecture

Use case diagrams

Use case diagrams to outline interactions between system users and the Credit Card Fraud Detection System. They depict various scenarios and user roles, including transaction monitoring, fraud investigation, and report generation, as shown in Figure 2.

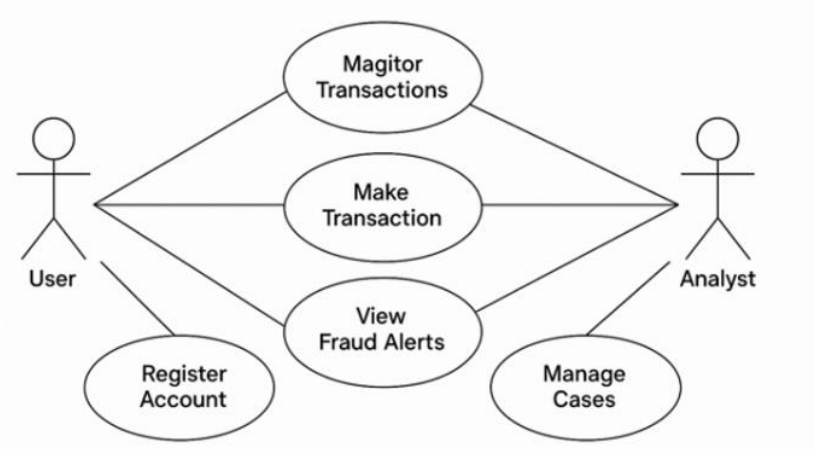

Figure 2: Use Case Diagram of web-based credit card fraud detection system

Entity Relationship Diagram (ERD)

An ERD visually represents the relationships between entities such as transactions, cardholders, users, fraud alerts, and cases. Figure 3 illustrates how data entities interact within the system to support fraud detection and prevention efforts.

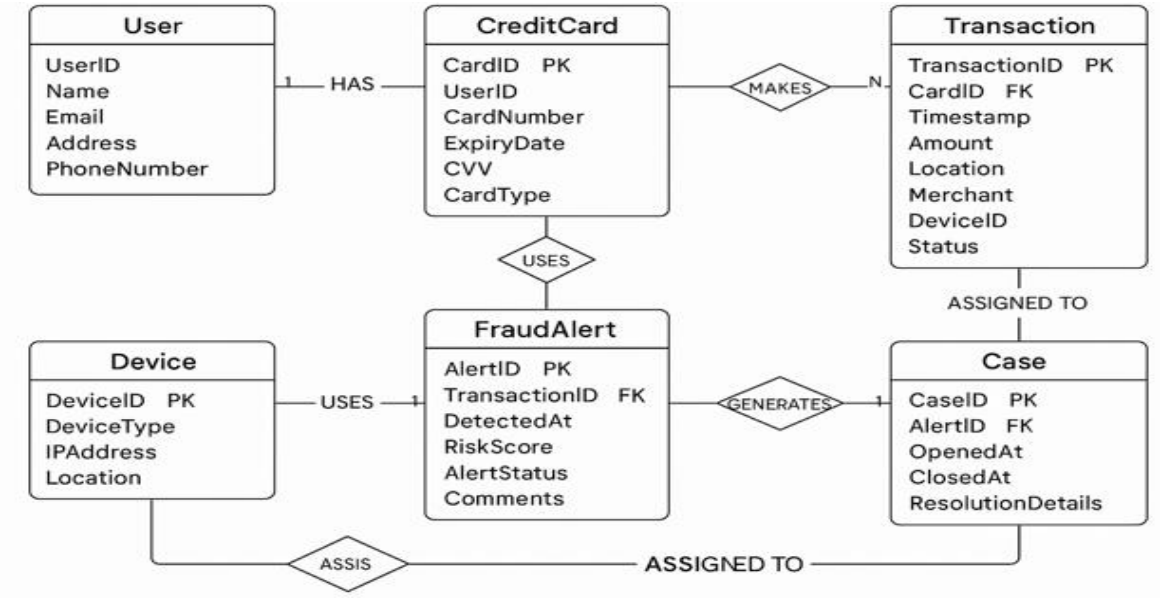

Figure3: Entity relationship diagram of web-based credit card fraud detection system

System Implementation

This section provides an overview of the technical tools used, and system testing procedures for the Credit Card Fraud Detection System.

Technical Tools Used

Python was chosen due to its extensive libraries and frameworks that are well-suited for data analysis and Pandas and NumPy were used to facilitate data manipulation and preprocessing. SQLite was used for its simplicity and integration with Python.

System Testing

Testing is crucial to ensure the Credit Card Fraud Detection System performs as expected and meets its functional requirements. It involves various testing types to identify and fix issues, ensuring system reliability and accuracy. For this study unit, both integration and functional testing are required to ensure the full functionality of the system. The unit testing of the system is illustrated in Table 2, integration testing in Table 3 and functionality testing respectively.

Table 2: Unit Testing

Test ID	Function	Description	Expected Result	Actual Result	Status
1	Transaction Monitoring	Test real-time transaction monitoring for fraud detection	System should flag suspicious transactions	Transactions were flagged correctly	Pass
2	Anomaly Detection	Test anomaly detection for transactions deviating from normal patterns	System should identify unusual transaction patterns	Anomalies were detected as expected	Pass
3	User Behavior Analysis	Test analysis of user behavior to detect deviations	System should detect deviations from established behavior profiles	Deviations were accurately detected	Pass

Table 2 focuses on testing individual components of the system. For example, tests were conducted on transaction monitoring, anomaly detection, and user behavior analysis. In each case, the system successfully flagged suspicious transactions, detected unusual patterns, and identified deviations from established user behaviors. These results confirm that the system's foundational functionalities are working.

Table 3: Integration Testing

Test ID	Function	Description	Expected Result	Actual Result	Status
1	Monitoring and Anomaly Detection	Test integration of real-time monitoring and anomaly detection	System should flag and analyze anomalies in real-time	System flagged and analyzed anomalies correctly	Pass
2	Data Source Integration	Test integration with external data sources	The system should use external data for enhanced fraud detection	External data was integrated successfully	Pass
3	Fraud Rules Engine	Test configuration of fraud detection rules	The system should apply rules and detect fraud according to the configured parameters	Fraud rules were applied correctly	Pass

Table 3 addresses the integration of various components within the system. This phase tested the integration between real-time monitoring and anomaly detection, the incorporation of external data sources, and the application of fraud detection rules. The system passed all these tests, indicating that the different modules interact seamlessly and the fraud detection rules are applied.

Table 4: Functionality Testing

Test ID	Function	Description	Expected Result	Actual Result	Status
1	End-to-End Functionality	Test end-to-end system functionality from transaction processing to fraud detection	The system should correctly process transactions and detect fraud	The system functioned as expected from start to end	Pass
2	Performance Testing	Test system performance under high transaction volumes	The system should handle high volumes without performance degradation	The system performed well under high loads	Pass
3	Security Testing	Test system security against potential threats	The system should protect against unauthorized access and data breaches	The system demonstrated robust security measures	Pass

Table 4 evaluates the overall performance and security of the system. Tests included end-to-end functionality, performance under high transaction volumes, and security against potential threats. The system successfully processed transactions, detected fraud, handled high loads without performance degradation, and demonstrated robust security measures. This confirms that the system is reliable and secure in a live environment.

Interfaces

This section describes the interfaces of the system. The system interfaces emphasis clarity, simple to use, easy to navigate, secure access to different system functions.

Login Page

The login screen allows authorized users to access the system securely, with roles defined for different user types as shown in Figure 4

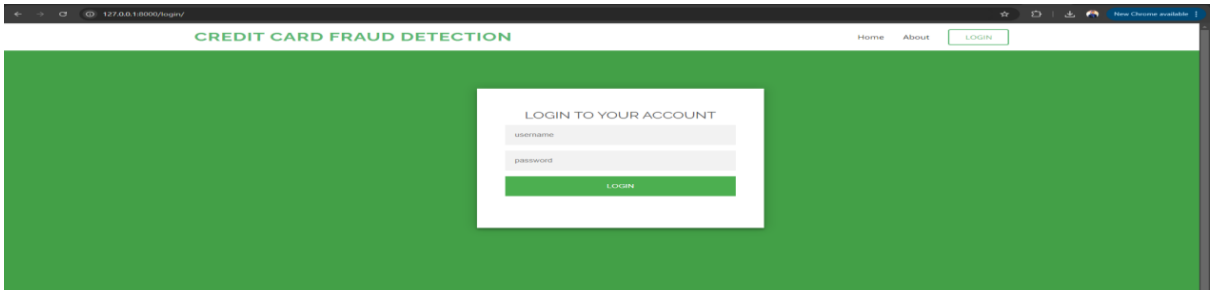

Figure 4: login page

Physical design

This provides a real-time view of transactions and alerts for any suspicious activities, as shown in Figure 5

Figure 5: Physical design

RESULTS AND DISCUSSION

Unit, integration, performance, and security tests were conducted on the system. Modules like transaction monitoring, anomaly detection, and user behavior analysis were verified to function properly through unit testing. The application of fraud rules and linkages to other data sources were among the components whose smooth operation was confirmed by integration testing. Security testing verified the system's resistance to injection threats and unauthorized access, while performance testing demonstrated that it could manage large transaction volumes without experiencing any deterioration. All things considered, the system operated dependably under controlled settings.

A number of restrictions surfaced, despite the results showing system dependability and functional success. This work did not conduct a thorough numerical evaluation of detection quality, in contrast to other works that report quantitative performance parameters including accuracy, precision, recall, and F1-score for fraud detection algorithms (Zou, 2024; Anjum et al., 2023). Opportunities for statistical benchmarking against current machine learning or hybrid methodologies were restricted by the dependence on rule-based detection logic.
Furthermore, it was more difficult to evaluate the results objectively in the previous draft due to the mixing of data and comments. Even if the system operated as intended, a clearer separation indicates that quantitative evaluation using benchmark datasets should be included in future studies to verify detection accuracy and reduce false positives. Comparative testing against pertinent approaches would also help place the contribution within the broader research environment.
rule-based and anomaly checks. Consequently, although the system exhibits potential as a useful web-based tool, its efficacy cannot yet be directly compared to cutting-edge models that record detection rates higher than 95%.

CONCLUSION

While maintaining system performance, security, and dependability, the web-based credit card fraud detection system demonstrated efficacy in detecting questionable transactions. Its primary contribution is a simple, useful framework for preventing fraud, although generalization is constrained by its reliance on static rules and controlled testing. To improve scalability and robustness, future improvements should include large-scale deployment, adaptive methods, and integration of external intelligence.

REFERENCE

Anjum, Prof. G., Pateriya, Prof. N., Thakre, Prof. N., Tiwari, A., & Mahanoor, S. (2023). Applying Machine Learning Techniques to Detect Credit Card Fraud. *International Journal of Innovative Research in Computer and Communication Engineering*, *11*(06), 8879–8883. https://doi.org/10.15680/ijircce.2023.1106074

Azeez, N. A., Idiakose, S. O., Onyema, C. J., & Vyver, C. Van Der. (2021). Cyberbullying Detection in Social Networks: Artificial Intelligence Approach. *Journal of Cyber Security and Mobility*, *10*(4), 745–774. https://doi.org/10.13052/jcsm2245-1439.1046

Beigi, S., & Amin-Naseri, M.-R. (2020). Credit Card Fraud Detection using Data mining and Statistical Methods. *Journal of AI and Data Mining*, *8*(2), 149–160. https://doi.org/10.22044/JADM.2019.7506.1894

Bolton, R. J., & Hand, D. J. (2001). *Unsupervised Profiling Methods for Fraud Detection*.

Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: opportunities, challenges, and fraud detection advancements. *Future Generation Computer Systems*, *158*, 410–426. https://doi.org/10.1016/J.FUTURE.2024.04.057

Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of Fraud Detection Techniques: Credit Card. In *International Journal of Computer Applications* (Vol. 45, Issue 1).

Chen, M. S., Han, J., & Yu, P. S. (1996). Data mining: An overview from a database perspective. In *IEEE Transactions on Knowledge and Data Engineering* (Vol. 8, Issue 6, pp. 866–883). https://doi.org/10.1109/69.553155

Chinazo Onyema, J., Ukamaka Betrand, C., & Benson-Emenike, M. (2023). *Machine Learning Credit Card Fraud Detection System* (Vol. 1, Issue 6).

Dhok, S. S. (2012). *Credit Card Fraud Detection Using Hidden Markov Model*.

Du, H., Lv, L., Guo, A., & Wang, H. (2023). AutoEncoder and LightGBM for Credit Card Fraud Detection Problems. *Symmetry*, *15*(4). https://doi.org/10.3390/sym15040870

Gao, J., Zhou, Z., Ai, J., Xia, B., & Coggeshall, S. (2019). Predicting Credit Card Transaction Fraud Using Machine Learning Algorithms. *Journal of Intelligent Learning Systems and Applications*, *11*(03), 33–63. https://doi.org/10.4236/jilsa.2019.113003

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems with Applications*, *193*, 116429. https://doi.org/10.1016/J.ESWA.2021.116429

Islam, S., Haque, M. M., & Karim, A. N. M. R. (2024). A rule-based machine learning model for financial fraud detection. *International Journal of Electrical and Computer Engineering*, *14*(1), 759–771. https://doi.org/10.11591/ijece.v14i1.pp759-771

Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. In *International Journal of Recent Technology and Engineering*. https://www.researchgate.net/publication/332264296

Karthik Meduri. (2024). Cybersecurity threats in banking: Unsupervised fraud detection analysis. *International Journal of Science and Research Archive*, *11*(2), 915–925. https://doi.org/10.30574/ijsra.2024.11.2.0505

Kotagiri, A. (2023). *Mastering Fraudulent Schemes: A Unified Framework for AI-Driven US Banking Fraud Detection and Prevention: ITAI Robotics process Automation Lead* (Vol. 7, Issue 7).

M.Dhavapriya, & Dr. V. Anuratha. (2024). *View of Credit Card Fraud Detection and Prevention In Point of Sale Using Apriori Algorithm*. https://publications.ngmc.ac.in/journal/index.php/arjst/article/view/13/18

Ogundunmade, T. P., & Adepoju, A. A. (2024). Modelling credit card fraud data using machine learning algorithms. *International Journal on Computational Engineering*, *1*(2), 43-49.

Olaniran, S. F., & Lawal, M. A. (2025). Addressing Class Imbalance in Credit Card Fraud Detection with Ensemble Learning and Domain-Specific Feature Engineering. *Journal of Basic and Applied Science Research*. https://doi.org/10.4314/jobasr.v3i5.7

Singh, H. (2024). Credit Card Fraud Detection. *International Journal for Research in Applied Science and Engineering Technology*, *12*(5), 2238–2244. https://doi.org/10.22214/ijraset.2024.62049

Zhu, X. J. (2005). Semi-supervised learning literature survey.

Zou, W. (2024). *A Comparative Analysis of Machine Learning Models for Credit Card Fraud Detection*. https://doi.org/10.54254/2754-1169/127/2024.OX18537