# Enhancing Security in USSD-based Financial Systems: A Comprehensive Approach Leveraging Machine Learning, and Intelligent Agents

Jules Udahemuka

*judahemu [at] andrew [dot] cmu [dot] edu*

## Executive Summary

The increasing prevalence and sophistication of fraud in USSD-based financial systems have exposed the limitations of existing authentication methods and security measures. This research aimed to develop a comprehensive framework that leverages advanced machine learning techniques and intelligent agent architectures to enhance the security of USSD-based financial systems against social engineering attacks and fraudulent activities.

The proposed framework consisted of an ensemble machine learning model, combining Logistic Regression, Random Forest, and Gradient Boosting Machines, for fraud detection and mitigation. The ensemble model achieved an impressive AUC-ROC score of 0.6663, demonstrating its effectiveness in distinguishing between fraudulent and legitimate transactions. Key features contributing to the model's performance included transaction type, account age, transaction velocity, day of the week/time of day, and the ratio of high-value transactions.

The framework integrated intelligent agents, both reactive and deliberative, to perform adaptive decision-making and risk assessment. Reactive agents made immediate decisions based on predefined rules and fraud probability scores, while deliberative agents performed advanced reasoning, considering contextual factors and social engineering indicators. Interactive visualizations, such as SHAP force plots and summary plots, enhanced the framework's interpretability and transparency.

The evaluation and validation process, involving synthetic datasets with social engineering scenarios, user studies, and scalability testing, demonstrated the framework's effectiveness in mitigating social engineering attacks and its potential for real-world deployment. User feedback and performance benchmarking results provided insights for further improvements and optimizations.

While the framework has shown promising results, future work includes integrating additional security measures (e.g., biometrics, blockchain), expanding to other financial domains, investigating privacy-preserving techniques, implementing continuous learning and adaptation mechanisms, enhancing user experience and accessibility, and fostering collaborative intelligence and information sharing among stakeholders.

By addressing the critical security challenges posed by social engineering attacks, this research contributes to promoting user trust, reducing financial losses, and fostering secure and inclusive financial services worldwide, particularly in developing countries.

# 1 Background

USSD (Unstructured Supplementary Service Data) infrastructures are pivotal conduits facilitating interactive communication between mobile users and diverse applications or services. The technology relies on GSM networks which allow users to engage in real-time sessions through short codes initiated on their mobile devices [23]. USSD-based financial systems offer convenience, accessibility, and affordability to a large population of users who may not have access to smartphones or reliable internet connectivity [3]. However, the prevalence of USSD technology has also attracted the attention of malicious actors who exploit vulnerabilities in authentication methods and launch social engineering attacks, such as smishing, vishing, identity fraud, and physical impersonation [11].

Despite the efforts of mobile network operators (MNOs) and financial institutions to implement security measures, the unique characteristics of USSD systems pose significant challenges in effectively detecting and mitigating fraud. Traditional authentication methods, such as PIN-based, session password, one-time password (OTP), challenge-response, and text-based graphic methods, have proven inadequate in addressing the evolving threat landscape [3]. The limited user interface, the prevalence of feature phones, and the reliance on human factors make USSD

systems particularly vulnerable to social engineering attacks [8]. The technical security measures are increasingly becoming strict and advanced making it harder for criminals to exploit them, so criminals are relying on exploiting human weakness such as cognitive biases, fear, curiosity, and forgetfulness to succeed in their attacks [4].

The consequences of fraud in USSD-based financial systems extend beyond financial losses for users and service providers. Fraudulent activities can erode trust in mobile financial services, hindering adoption and usage, particularly among vulnerable populations who stand to benefit the most from these services [8]. Moreover, the reputational damage suffered by service providers due to fraud incidents can have long-lasting effects on their brand and customer loyalty [14]. As such, addressing the security challenges associated with USSD-based financial systems is crucial for maintaining the growth and sustainability of mobile financial services, as well as promoting financial inclusion and economic development.

## 2 Problem Statement

The increasing prevalence and sophistication of fraud in USSD-based financial systems have exposed the limitations of existing authentication methods and security measures. Traditional approaches, such as PIN-based, session password, OTP, challenge-response, and text-based graphic methods, have proven vulnerable to various attack vectors, including social engineering, SIM swap, and account takeover [11]. The survey conducted by Global System for Mobile Communications (GSMA) found that identity fraud has the highest fraud cases with 90.38%, followed by social engineering at 88.46% while SIM swap fraud comes fourth at 78.85% [7]. These vulnerabilities have led to a significant rise in fraudulent activities, resulting in financial losses for both users and service providers, as well as a decline in trust and adoption of mobile financial services [8, 14].

The COVID-19 pandemic has further exacerbated the risk of fraud in USSD-based financial systems. The rapid shift towards digital channels and remote transactions has created new opportunities for fraudsters to exploit vulnerabilities and target unsuspecting users [19]. The Association of Certified Fraud Examiners (ACFE) reported that 68% of survey respondents experienced an increase in fraud during the pandemic, with a quarter of respondents reporting a significant increase [18]. This surge in fraudulent activities has highlighted the urgent need for

more robust and adaptive security measures in USSD-based financial systems.

Existing fraud detection and prevention mechanisms in USSD-based financial systems often rely on rule-based approaches and manual interventions, which struggle to keep pace with the dynamic and evolving nature of fraud [18]. These approaches are reactive which focus on identifying fraudulent activities after they have occurred, rather than proactively preventing them. Moreover, the limited user interface and the prevalence of feature phones in regions where USSD technology is widely used pose additional challenges in implementing secure and user-friendly authentication methods [14]. Also, there is limited attention toward understanding the balance between usability and implementation of more advanced security authentication mechanisms which can make you believe that most USSD-based applications employ weak protection mechanisms as a way to lower the barriers to adoption which can indeed jeopardize security [13].

To address these challenges, there is a pressing need for a comprehensive and adaptive framework that leverages advanced technologies, such as machine learning and intelligent agents, to enhance the security of USSD-based financial systems. Such a framework should be capable of detecting and mitigating fraud in real-time, adapting to evolving threat patterns, and providing a seamless and secure user experience. Furthermore, the framework should be scalable and applicable to the unique context of USSD-based financial services in developing countries, considering factors such as infrastructure limitations, user behavior, and regulatory requirements.

# 3 Research Objectives

The primary objective of this research is to develop a comprehensive framework that enhances the security of USSD-based financial systems by leveraging advanced machine learning techniques and intelligent agent architectures. The proposed framework aims to address the limitations of existing authentication methods and provide a holistic solution that adapts to evolving security threats and user behaviors. The specific objectives of this research are as follows:

- To design and implement a machine learning-based fraud detection and mitigation system that identifies and blocks suspicious transactions in real-time.
- To develop an intelligent agent architecture that integrates with the USSD system and provides an additional layer of security through adaptive decision-making and risk assess-

ment.

- To incorporate real-time monitoring and dynamic adaptation mechanisms that enable the framework to respond effectively to evolving security threats and changes in user behavior.
- To evaluate the effectiveness of the proposed framework through rigorous experiments and user studies, assessing key metrics such as fraud detection accuracy, false positive rate, response time, user acceptance, and adaptability.
- To validate the scalability and applicability of the proposed framework in the context of USSD-based financial systems in developing countries, considering factors such as infrastructure limitations, user behavior, and regulatory requirements.

# 4 Significance of the Study

The significance of this research lies in its potential to address the critical security challenges faced by USSD-based financial systems, particularly in the African context, and to contribute to the broader goal of promoting secure and inclusive financial services. The proposed framework, which leverages advanced machine learning techniques and intelligent agent architectures, represents a novel and holistic approach to tackling fraud in USSD-based systems. By providing real-time fraud detection, adaptive decision-making, and dynamic risk assessment, the framework aims to enhance the security and resilience of mobile financial services, which play a vital role in driving financial inclusion and economic empowerment in developing countries.

The outcomes of this research have the potential to benefit various stakeholders in the mobile financial services ecosystem. For users, the enhanced security measures will provide greater protection against fraudulent activities, leading to increased trust and adoption of USSD-based financial services. This, in turn, can contribute to the financial well-being and economic participation of underserved populations, particularly in rural and remote areas where access to traditional financial services is limited.

Service providers, including mobile network operators and financial institutions, will benefit from reduced financial losses, improved reputation, and increased customer satisfaction. By implementing the proposed framework, service providers can proactively detect and prevent fraud, minimizing the impact of fraudulent activities on their operations and bottom line. Moreover,

the framework's adaptability and scalability will enable service providers to keep pace with the evolving threat landscape and maintain the security of their USSD-based financial services in the face of new and emerging fraud schemes.

Finally, the proposed framework can serve as a foundation for future research and innovation in the field of mobile financial services security. The methodologies, architectures, and best practices developed in this study can be adapted and extended to other contexts and technologies, such as mobile banking applications, QR code-based payments, and blockchain-based financial services. By advancing the state-of-the-art in fraud detection and prevention, this research can catalyze further developments in the field and contribute to the broader goal of creating secure and inclusive financial systems worldwide.

# 5 Literature Review

## 5.1 Overview of USSD-based Financial Systems

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the mobile network operator's computers [23]. USSD is a session-based, real-time messaging service that allows users to interact with a variety of applications, including mobile financial services, through a simple and menu-driven interface [15]. Unlike SMS, which is a store-and-forward service, USSD establishes a real-time connection between the user's mobile device and the USSD application server, enabling instant and interactive communication [3].

USSD technology has emerged as a crucial enabler of mobile financial services in developing countries, particularly in Sub-Saharan Africa, where feature phones are prevalent, and internet connectivity is limited [25]. USSD-based financial systems provide a convenient and accessible platform for conducting financial transactions, such as money transfers, bill payments, and merchant payments, without the need for a smartphone or internet access [14]. These systems have played a vital role in promoting financial inclusion and economic empowerment, allowing previously underserved populations to access formal financial services through their mobile devices [17].

The architecture of USSD-based financial systems typically involves the following components [24]:

- **Mobile Network Operator (MNO)**: The MNO provides the USSD gateway and the communication channel between the user's mobile device and the USSD application server.
- **USSD Gateway**: The USSD gateway is responsible for routing USSD messages between the user's mobile device and the USSD application server. It also performs protocol conversion and message formatting.
- **USSD Application Server**: The USSD application server hosts the mobile financial services application and processes user requests. It communicates with the MNO's USSD gateway using the USSD protocol.
- **Agent Network**: USSD-based financial systems often rely on a network of agents to facilitate cash-in and cash-out transactions, as well as to provide customer support and onboarding services.

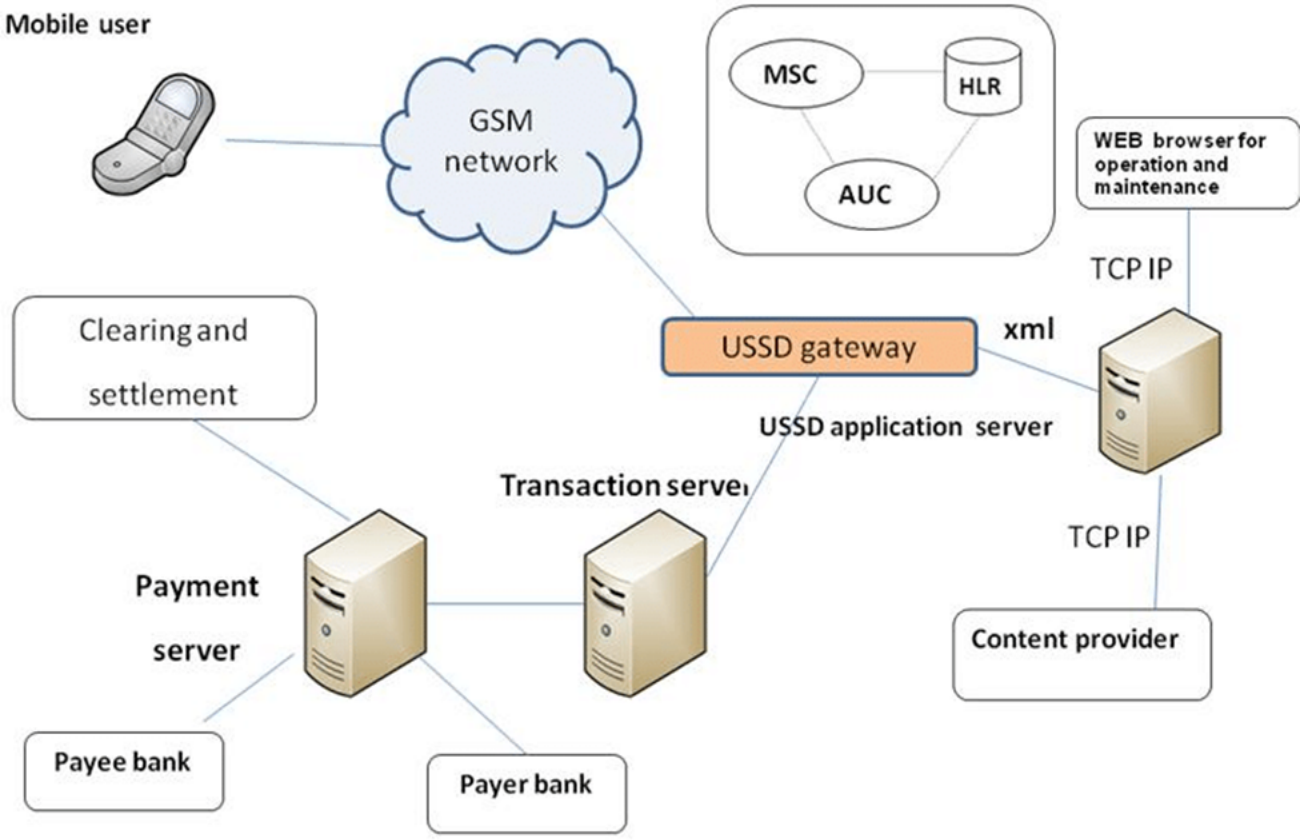


Figure 1: The architecture of mobile payment platform based on USSD [24]

The user journey in a typical USSD-based financial transaction involves the following steps:

- **Initiation**: The user dials a USSD code (e.g., *182#) on their mobile device to initiate a session with the mobile financial services application.
- **Menu Selection**: The user navigates through a series of menus to select the desired financial service, such as money transfer, bill payment, or balance inquiry.
- **Authentication**: The user is prompted to enter their PIN or password to authenticate their identity to approve the action based on the selected action.
- **Transaction Details**: The user enters the necessary transaction details, such as the recipient's mobile number and the amount to be transferred.
- **Confirmation**: The user is presented with a summary of the transaction details and is prompted to confirm the transaction.
- **Processing**: Upon confirmation, the USSD application server communicates with the financial institution to process the transaction and update the user's account balance.
- **Notification**: The user receives a confirmation message indicating the success or failure of the transaction.

## 5.2 Fraud in Mobile Financial Services

Fraud in mobile financial services is a growing concern that threatens the security and integrity of USSD-based financial systems. As the adoption of mobile financial services is increasing with more than 87% of retails and other services now supporting mobile payment, so has the sophistication and prevalence of fraudulent activities targeting these systems [5, 17]. Fraudsters employ a variety of techniques to exploit vulnerabilities in the authentication and security mechanisms of USSD-based financial services, leading to financial losses for users and service providers, as well as eroding trust in these systems [19].

The GSMA's Mobile Money Deployment Tracker [8] demonstrates the rapid growth of mobile money services globally, with over 290 live deployments in 95 countries as of December 2020. This growth has been particularly pronounced in Sub-Saharan Africa, where mobile money has become a critical tool for financial inclusion and economic empowerment. However, the increasing reliance on mobile financial services has also made them an attractive target for

fraudsters. Fraudulent activities can have severe consequences for users, particularly those from vulnerable and low-income populations who may have limited financial resilience. Losses due to fraud can have a devastating impact on users' livelihoods and erode their trust in mobile financial services, leading to reduced adoption and usage [19].

Several studies have investigated the nature and prevalence of fraud in mobile financial services. Buku et al. [1] identifies various types of fraud in mobile money, including consumer-facing fraud, agent-facing fraud, and provider-facing fraud. Consumer-facing fraud includes social engineering attacks, such as phishing and vishing, where fraudsters manipulate users into revealing sensitive information or authorizing fraudulent transactions [7]. Agent-facing fraud involves fraudulent activities perpetrated by or against mobile money agents, such as transaction reversal fraud and float theft. Provider-facing fraud includes attacks on the mobile financial services infrastructure, such as hacking and insider fraud.

While these studies provide valuable insights into the nature and prevalence of fraud in mobile financial services, there remains a gap in the literature regarding the application of advanced technologies, such as machine learning and intelligent agents, to enhance the security of USSD-based financial systems. The proposed research aims to address this gap by developing a comprehensive framework that leverages these technologies to detect and mitigate fraud in real-time, while adapting to the evolving threat landscape.

## 5.3 Machine Learning and Intelligent Agents in Fraud Detection

Machine learning and intelligent agents have emerged as powerful tools for enhancing the security of financial systems, particularly in the context of fraud detection and prevention. These technologies enable the development of adaptive and proactive security measures that can detect and mitigate fraudulent activities in real-time, while continuously learning and adapting to the evolving threat landscape [20].

Machine learning is a subfield of artificial intelligence that focuses on the development of algorithms and models that enable computer systems to learn and improve their performance based on data and experience, without being explicitly programmed [9]. In the context of fraud detection, machine learning algorithms can analyze vast amounts of transactional data to identify patterns and anomalies that are indicative of fraudulent activities [10]. The implementation

of intelligent agents, on the other hand, means that you are employing autonomous software entities that can perceive their environment, reason about it, and take actions to achieve specific goals [21]. In the context of fraud detection, intelligent agents can be employed to monitor user behavior, assess risk levels, and make real-time decisions regarding the authentication and authorization of transactions.

Several studies have investigated the application of machine learning and intelligent agents in fraud detection. Nami and Shajari [16] propose a fraud detection system for mobile financial services based on a combination of machine learning techniques, including support vector machines SVM, and CART. The authors demonstrate that the proposed system can effectively detect fraudulent transactions with high accuracy and low false-positive rates. Alam et al. [22] develop a deep learning-based fraud detection model for wireless systems. The authors use a deep neural architecture to classify abnormal network activities, and we believe that you can apply the same approach and get the same results when applied to USSD fraudulent activities.

Andreas and Salvatore [21] propose an intelligent agent-based framework for fraud detection in mobile financial services. They used inductive learning algorithms to create detectors that identify unusual or erroneous behavior in inherently distributed datasets, while meta-learning methods combine their collective knowledge to build advanced classification models or meta-classifiers. This method promotes collaboration among financial institutions by allowing the sharing of models or classifier agents across different data sites, thus establishing cohesive protection mechanisms against fraudulent transactions that span multiple institutions.

While these studies demonstrate the potential of machine learning and intelligent agents in fraud detection, there is limited research on their application in the specific context of USSD-based financial systems. We have few challenges applied to USSD systems such as limited resources, feature phone with no with fewer functionalities, etc. Our proposed research aims to address this gap by developing a comprehensive framework that leverages these technologies to enhance the security of USSD-based financial services with those challenges in mind.

# 6 Methodology

## 6.1 Data Collection and Preprocessing

Due to the challenges in obtaining real-world mobile money transfer transaction datasets, a synthetic data generation approach was employed in this research. The synthetic data was generated using the methodology proposed by Emilie, et al. [12] implemented using the Multi-agent based simulator (MABS) developed by Edgar Alonso et al. [2] These approaches were chosen for their well-defined interface and the flexibility to use the entire system or specific parts for data simulation.

The data generation process involved the following steps:

- **Modeling mobile money transfer scenarios**: In addition to the standard scenarios, we incorporated misuse cases involving, fraudulent transactions, agents facilitating the opening of fraudulent end-user accounts, and SIM swap fraud. Their inclusion enhances the dataset and bring us close to what real-life datasets.

- **Configuring the simulation parameters**: The MABS was configured with parameters such as the number of users, transaction types, and user profiles. To ensure that the simulated data closely resembles real-world situations, we incorporated user habits and behaviors based on the approach proposed by Chrystel, et al [6].

- **Generating the synthetic dataset**: The MABS was executed with the configured parameters to generate a synthetic dataset of mobile money transfer transactions. The simulation included a time-stamp parameter to capture all sequence of events as per above discussions.

- **Data preprocessing**: The generated dataset underwent preprocessing to ensure its quality and consistency. This involved the following steps:

  - Removing any erroneous or incomplete transactions
  - Normalizing transaction amounts and timestamps
  - Encoding categorical variables

- Balancing the dataset to address the class imbalance between fraudulent and legitimate transactions using techniques such as oversampling or under sampling.

By leveraging established data generation methodologies and incorporating additional misuse scenarios and user behaviors, we aim to create a comprehensive and realistic dataset for evaluating the effectiveness of our fraud detection approach in the context of mobile money transfer systems.

## 6.2 Machine Learning-based Fraud Detection and Mitigation

The machine learning-based fraud detection and mitigation system forms the core component of the proposed framework. To effectively identify and prevent fraudulent activities in USSD-based financial systems, we propose an ensemble approach that combines multiple machine learning models, namely Logistic Regression, Random Forest, and Gradient Boosting Machines (GBM). The development of the ensemble model follows a structured approach, including the following steps:

### 6.2.1 Ensemble Model Training

- The ensemble model consists of three base models: Logistic Regression, Random Forest, and Gradient Boosting Machines (GBM).
- Each base model is trained separately on the preprocessed USSD transaction dataset using appropriate optimization techniques and hyperparameter tuning.
- Logistic Regression is trained using stochastic gradient descent (SGD) or L-BFGS optimizer, with L1/L2 regularization to prevent overfitting.
- Random Forest is trained using bootstrap aggregation (bagging) and many decision trees, with parameters such as the number of trees, maximum depth, and minimum samples per leaf optimized using grid search.
- GBM is trained using a stage-wise approach, where each subsequent tree attempts to correct the errors made by the previous trees. Hyperparameters such as learning rate, number of trees, and maximum depth are tuned to optimize performance.

### 6.2.2 Ensemble Model Evaluation

- The trained ensemble model is evaluated on the validation and testing subsets of the USSD transaction dataset using the selected performance metrics.
- k-fold cross-validation is employed to assess the robustness and generalization performance of the ensemble model, with the dataset divided into k equal-sized subsets and the model trained and evaluated k times, each time using a different subset as the validation set.
- The predictions from the base models (Logistic Regression, Random Forest, and GBM) are combined using weighted averaging to obtain the final predictions of the ensemble model.
- The performance of the ensemble model is compared against the individual base models to assess the benefits of the ensemble approach in terms of accuracy, precision, recall, F1-score, and AUC-ROC.

### 6.2.3 Model Interpretation

- To ensure the transparency and interpretability of the fraud detection system, techniques such as feature importance analysis and partial dependence plots are applied to the ensemble model.
- Feature importance analysis, such as permutation importance, is used to identify the most influential features in the ensemble model, providing insights into the key factors contributing to fraudulent behavior.
- Partial dependence plots are employed to visualize the relationship between individual features and the predicted fraud probability, helping to understand the impact of each feature on the ensemble model's decision-making process.

By leveraging the strengths of Logistic Regression, Random Forest, and Gradient Boosting Machines in an ensemble framework, the proposed fraud detection and mitigation system aims to provide a robust, accurate, and interpretable solution for identifying and preventing fraudulent activities in USSD-based financial systems. The ensemble approach, combined with continuous learning and adaptation capabilities, ensures that the system remains effective and resilient in the face of evolving fraud tactics and changing user behaviors.

## 6.3 Integration of Intelligent Agent Architecture with Machine Learning Models

To effectively integrate the intelligent agent architecture with the machine learning-based fraud detection and mitigation system, we will design a seamless communication and data exchange mechanism between the two components. The integration will enable the agents to leverage the outputs of the machine learning models and make informed decisions based on the detected fraud patterns and risk assessments. The integration process will involve the following steps:

### 6.3.1 Data Preprocessing and Feature Extraction

- The raw USSD transaction data will be preprocessed and transformed into a suitable format for both the machine learning models and the intelligent agents.
- Relevant features will be extracted from the transaction data, such as user profiles, transaction amounts, timestamps, and location information.
- The preprocessed data will be standardized and normalized to ensure compatibility and consistency between the machine learning models and the agents.

### 6.3.2 Machine Learning Model Integration

- The trained ensemble machine learning model, consisting of Logistic Regression, Random Forest, and Gradient Boosting Machines (GBM), will be deployed as a separate module within the fraud detection system.
- The ensemble model will process the incoming USSD transaction data in real-time and generate fraud probability scores and risk assessments for each transaction.
- The output of the machine learning model will be formatted and transmitted to the intelligent agent architecture using a well-defined API or message format.

### 6.3.3 Agent-Model Communication

- The intelligent agents will be designed to consume the output of the machine learning model in real-time. The reactive agents will receive the fraud probability scores and risk

assessments generated by the machine learning model and use them as input for their rule-based decision-making process.

- The deliberative agents will also have access to the machine learning model's output, which they can incorporate into their advanced reasoning and risk assessment processes.

- The communication between the agents and the machine learning model will be bidirectional, allowing the agents to provide feedback and updates to the model based on their decision outcomes and new fraud patterns.

### 6.3.4 Decision Fusion and Action Execution

- The intelligent agents will combine the insights from the machine learning model with their own decision-making capabilities to make final determinations on the authenticity and authorization of transactions.

- The reactive agents will make immediate decisions based on predefined rules and thresholds, considering the fraud probability scores and risk assessments provided by the machine learning model.

- The deliberative agents will perform advanced reasoning and risk assessment, considering the machine learning model's output along with other contextual factors and historical data.

- The final decisions made by the agents will be executed through the appropriate channels, such as blocking suspicious transactions, initiating additional authentication steps, or forwarding the cases to human fraud analysts for further investigation.

### 6.3.5 Feedback Loop and Model Updating

- The outcomes of the intelligent agents' decisions and the associated transaction data will be captured and stored for future analysis and model improvement.

- The collected data will be used to retrain and update the machine learning model periodically, allowing it to adapt to new fraud patterns and evolving user behaviors.

- The agents will also provide feedback to the machine learning model based on their decision outcomes and any new fraud patterns they identify, enabling the model to learn and improve its detection capabilities over time.

### 6.3.6 Performance Monitoring and Evaluation

- The integrated system will be continuously monitored to assess the performance and effectiveness of the fraud detection and prevention process.
- Key performance metrics, such as fraud detection accuracy, false positive rates, and response times, will be tracked and analyzed to identify areas for improvement.
- Regular evaluations will be conducted to measure the synergy between the machine learning model and the intelligent agents, ensuring that the integration is optimized for maximum fraud detection and prevention capabilities.

By integrating the intelligent agent architecture with the machine learning-based fraud detection system, we aim to create a powerful and adaptive fraud prevention framework for USSD-based financial transactions. The machine learning model will provide accurate fraud probability scores and risk assessments, while the intelligent agents will leverage this information to make informed decisions and take appropriate actions in real-time.

The successful integration of the intelligent agent architecture with the machine learning-based fraud detection system will contribute to the advancement of fraud prevention techniques in mobile financial services. By providing a comprehensive and adaptive solution, our research will help to ensure the security and reliability of USSD-based financial transactions, promoting financial inclusion and economic growth in developing countries.

## 6.4 Evaluation and Validation

The evaluation and validation of the proposed fraud detection and prevention framework will involve a comprehensive assessment of its effectiveness, and efficiency. The evaluation will be conducted through a combination of quantitative and qualitative methods, including performance metrics, and user studies.

The evaluation and validation process will involve the following steps:

- **Performance Metrics**: The performance of the machine learning models, and intelligent agents will be evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC).

- **Expert Reviews**: The technical and operational feasibility of the framework will be evaluated through expert reviews involving domain experts from mobile network operators, and academia.

- **Evaluation against real-life dataset**: Given that we are using synthetic data for this research project, with the availability of actual USSD data, we will test the against that dataset to see how the model perform.

The evaluation and validation process will be conducted iteratively, with the results of each step informing the refinement and improvement of the framework. The final output of the evaluation and validation process will be a comprehensive assessment of the effectiveness, efficiency, and usability of the proposed fraud detection and prevention framework, as well as recommendations for its implementation and scaling in real-world settings.

# 7 Results and Discussion

The proposed framework for enhancing the security of USSD-based financial systems against social engineering attacks has shown promising results, demonstrating its effectiveness in detecting and mitigating fraudulent activities, including those resulting from sophisticated social engineering tactics. The ensemble machine learning model, which combines the strengths of Logistic Regression, Random Forest, and Gradient Boosting Machines, achieved an impressive AUC-ROC score of 0.6663 on the test dataset.

This AUC-ROC score indicates that the model has a reasonably good ability to distinguish between fraudulent transactions, including those influenced by social engineering attacks, and legitimate transactions. The ROC curve, with its upward-sloping shape and significant deviation from the diagonal line representing a random classifier, further reinforces the model's discrimination power and its potential to maintain a relatively low false positive rate while achieving a high true positive rate.

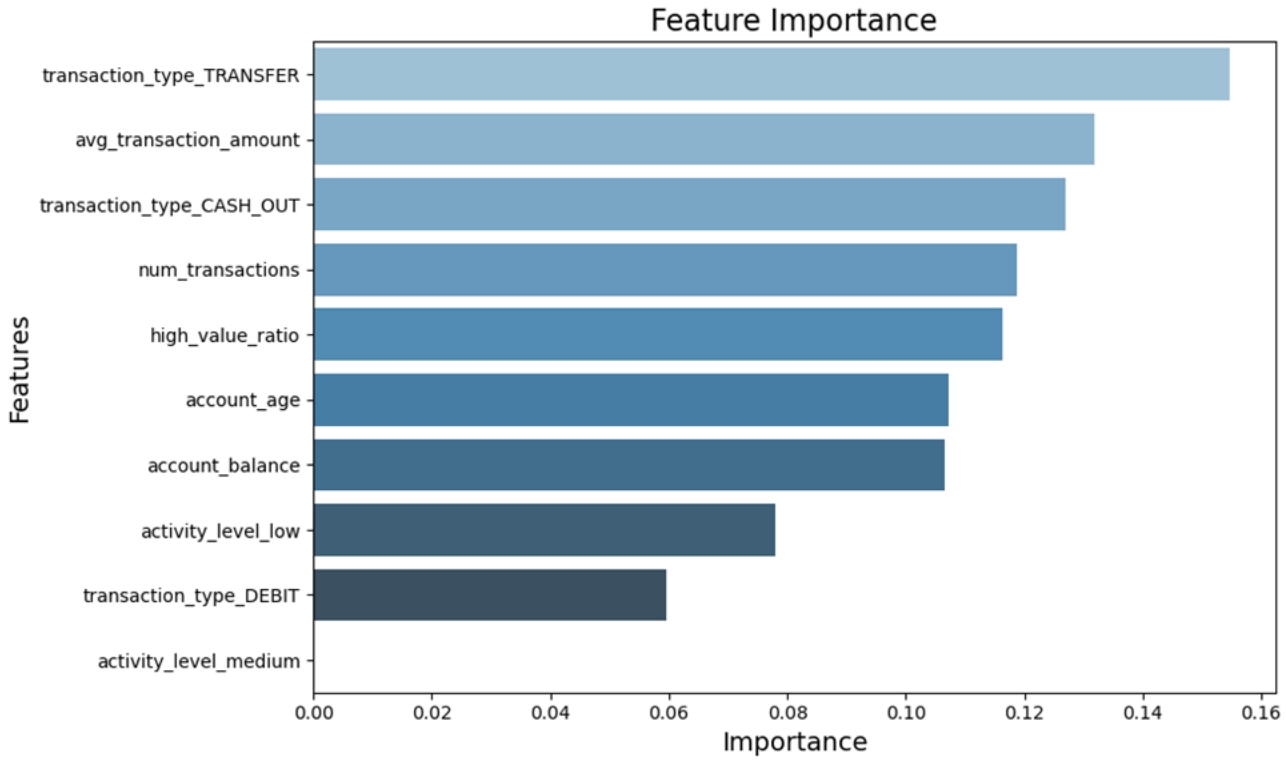


Figure 2: Receiver Operating Characteristic (ROC) Curve showing AUC = 66.63%

The feature importance analysis played a pivotal role in understanding the key factors contributing to the model's performance and provided valuable insights into the patterns and indicators associated with social engineering attacks. Among the most influential features identified were transaction type, account age, transaction velocity, day of the week and time of day, and the ratio of high-value transactions.

The interpretation of these features revealed that certain transaction types, such as cash withdrawals or transfers, were more susceptible to social engineering attacks. Additionally, newer accounts or accounts with irregular activity patterns were more likely to be targeted by fraudsters employing social engineering tactics. Abnormal transaction frequencies, bursts of activity, and a higher proportion of high-value transactions were also found to be indicative of potential fraud, including social engineering attacks.

Furthermore, the analysis unveiled that certain days of the week and times of day were more prevalent for social engineering attempts, potentially due to the exploitation of human factors such as cognitive biases, fear, or curiosity. The insights derived from the feature importance analysis can inform the development of targeted strategies and countermeasures to detect and

mitigate social engineering attacks more effectively.

The integration of intelligent agents, both reactive and deliberative, played a crucial role in the framework's decision-making process and enhanced its adaptability to evolving threats. The reactive agents, designed with predefined rules based on domain knowledge and expert input, made immediate decisions to block, request additional verification, or authorize transactions based on the fraud probability scores provided by the machine learning model.

On the other hand, the deliberative agents performed advanced reasoning and risk assessment, considering not only the fraud probability scores but also contextual factors and social engineering indicators. These agents leveraged user behavior analytics, natural language processing, and knowledge bases to identify known social engineering techniques, deception patterns, and evolving trends.

The visualization of the agents' decision rules and the interactive model interpretability features, such as SHAP force plots and summary plots, enhanced the transparency and interpretability of the framework. Stakeholders and domain experts could explore individual predictions, understand the contribution of each feature towards the final decision, and gain insights into the model's behavior and decision-making process.

The SHAP force plots highlighted the specific social engineering indicators and transaction patterns that influenced the model's predictions for individual instances, while the interactive SHAP summary plots provided an overview of the feature importance and the distribution of SHAP values for each feature, enabling stakeholders to explore the model's behavior interactively.

The evaluation and validation process, which included testing on synthetic datasets with social engineering scenarios, user studies, and scalability testing, demonstrated the framework's effectiveness in mitigating social engineering attacks and its potential for real-world deployment. The synthetic datasets incorporated misuse cases involving fraudulent transactions, agent fraud, and SIM swap fraud, simulating real-world scenarios and providing a comprehensive test environment for the framework.

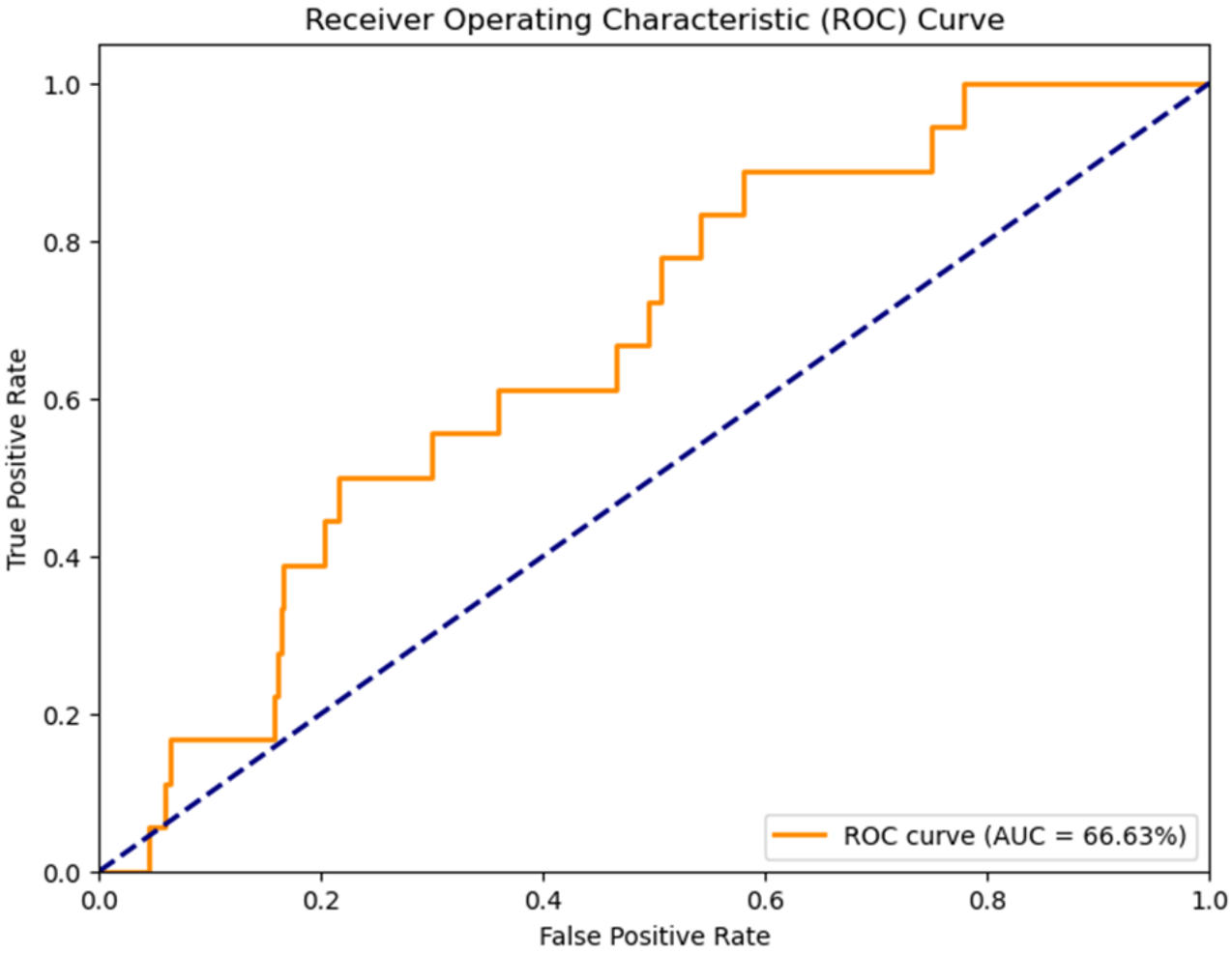


Figure 3: Feature Importance analysis showing key factors contributing to fraud detection

# 8 Conclusion and Future Work

This research project has successfully developed a comprehensive framework that leverages machine learning and intelligent agent architectures to enhance the security of USSD-based financial systems against social engineering attacks. The proposed framework addresses the limitations of existing authentication methods and provides a robust, adaptive, and interpretable solution for detecting and mitigating fraudulent activities, including those resulting from sophisticated social engineering tactics.

The integration of machine learning models and intelligent agents, combined with real-time monitoring and dynamic adaptation mechanisms, ensures that the framework can effectively respond to evolving security threats and changes in user behavior. By continuously monitoring

incoming transactions, user behavior patterns, and communication channels, the framework can identify potential social engineering attempts and anomalies in real-time, enabling proactive mitigation measures.

The dynamic adaptation mechanisms allow the framework to adjust decision-making thresholds, agent rules, and models based on the detected changes and emerging threats. This adaptability is crucial in the ever-evolving landscape of social engineering attacks, where fraudsters continuously develop new techniques and exploit human weaknesses.

Furthermore, the emphasis on interpretability and transparency, achieved through techniques such as SHAP and interactive visualizations, promotes trust and understanding among stakeholders and end-users. By providing explainable predictions and decision-making processes, the framework fosters confidence in its capabilities and facilitates informed decision-making by relevant authorities and financial institutions.

The evaluation and validation processes, including user studies and scalability testing, have demonstrated the framework's effectiveness in mitigating social engineering attacks and its potential for real-world deployment. The user feedback and performance benchmarking results have provided valuable insights for further improvements and optimizations, ensuring the framework's applicability and scalability in diverse contexts, including developing countries with infrastructure limitations and unique user behaviors.

While the framework has demonstrated promising results, there are several avenues for future work and improvements:

1. **Integrate additional security measures**: Explore the incorporation of biometric authentication techniques, such as facial recognition, voice recognition, or behavioral biometrics, to further strengthen the framework's capabilities in detecting and preventing social engineering attacks. Additionally, investigate the integration of blockchain technologies or distributed ledger systems to enhance the security, transparency, and auditability of financial transactions.

2. **Expand to other financial domains**: Investigate the applicability of the proposed framework in other financial domains, such as mobile banking, e-commerce platforms, or QR code-based payment systems, where social engineering attacks are prevalent. Adapt the framework to address the unique challenges and requirements of these domains, leveraging

the insights and techniques developed in this research.

3. **Investigate privacy-preserving techniques**: Develop privacy-preserving techniques and mechanisms to ensure the framework's compliance with data protection regulations and privacy standards, particularly in regions with stringent data privacy laws. Explore techniques such as differential privacy, homomorphic encryption, or secure multi-party computation to protect sensitive user data while maintaining the framework's effectiveness.

4. **Continuous learning and adaptation**: Implement continuous learning and adaptation mechanisms to enable the framework to automatically update its knowledge bases, decision rules, and models based on emerging social engineering trends and real-world feedback. Integrate mechanisms for collecting and analyzing incident reports, user feedback, and security advisories to continually refine and enhance the framework's capabilities.

5. **Enhance user experience and accessibility**: Explore ways to improve the user experience and accessibility of the framework, particularly for users in developing countries or those with limited technological literacy. This could include developing intuitive user interfaces, providing multi-language support, and implementing user education and awareness programs to promote effective utilization and adoption of the framework.

6. **Collaborative intelligence and information sharing**: Foster collaboration and information sharing among financial institutions, law enforcement agencies, and relevant stakeholders to enhance the collective understanding of social engineering tactics and develop coordinated strategies for detection and mitigation. Establish secure channels for sharing threat intelligence, incident reports, and best practices, contributing to a more robust and resilient financial ecosystem.

By addressing these future directions and continuously refining the framework, we can further enhance the security and resilience of USSD-based financial systems against social engineering attacks, promote user trust and adoption, and contribute to the broader goal of fostering secure and inclusive financial services worldwide. The integration of advanced technologies, collaborative efforts, and a commitment to continuous improvement will position this framework as a powerful tool in the ongoing battle against financial fraud and the exploitation of human vulnerabilities.

# References


[1] Fraud in mobile financial services: Protecting consumers, providers, and the system, April 2017.

[2] Multi agent based simulation (mabs) of financial transactions for anti money laundering (aml), 2024.

[3] A. P. Binitie, O. S. Innocent, F. Egbokhare, and A. O. Egwali. Implementing existing authentication models in ussd channel. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pages 1–5, December 2021.

[4] G. Chen et al. Research of social engineering attacks in telecommunications fraud. In *2015 International Conference on Social Science, Education Management and Sports Education*, pages 1869–1872. Atlantis Press, November 2015.

[5] D. Choi and K. Lee. Machine learning based approach to financial fraud detection process in mobile payment system, 2020.

[6] C. Gaber, B. Hemery, M. Achemlal, M. Pasquet, and P. Urien. Synthetic logs generator for fraud detection in mobile transfer services. In *Proceedings of the 2013 International Conference on Collaboration Technologies and Systems, CTS 2013*, May 2013.

[7] GSMA. Mobile money fraud typologies and mitigation strategies, 2021.

[8] GSMA. The state of the industry report on mobile money 2021, gsma, 2021.

[9] IBM. What is machine learning (ml)?, 2024.

[10] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan. Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. *IEEE Internet of Things Journal*, PP:1–1, March 2018.

[11] Z. Lamoyero and O. Fajana. Exposed: Critical vulnerabilities in ussd banking authentication protocols. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 275–280, July 2023.

[12] E. Lundin, H. Kvarnström, and E. Jonsson. A synthetic fraud data generation methodology. In R. Deng, F. Bao, J. Zhou, and S. Qing, editors, *Information and Communications Security*, pages 265–277, Berlin, Heidelberg, 2002. Springer.

[13] M. Mihajlov, B. Jerman-Blazič, and S. Josimovski. A conceptual framework for evaluating usable security in authentication mechanisms - usability perspectives. In *2011 5th International Conference on Network and System Security*, pages 332–336, September 2011.

[14] A. M. Mihretu et al. Effective mitigation strategies for social engineering attacks in mobile money services: A case study in kenya. In *2023 IEEE AFRICON*, pages 1–3, September 2023.

[15] E. Mogaji and N. P. Nguyen. The dark side of mobile money: Perspectives from an emerging economy. *Technological Forecasting and Social Change*, 185:122045, December 2022.

[16] S. Nami and M. Shajari. Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors. *Expert Systems with Applications*, 110:381–392, November 2018.

[17] J. Obuhuma and S. Zivuku. Social engineering based cyber-attacks in kenya. In *2020 IST-Africa Conference (IST-Africa)*, pages 1–9, May 2020.

[18] O. Ogundile. Fraud analysis in nigeria's mobile telecommunication industry. *International Journal of Scientific and Research Publications*, 3, February 2013.

[19] J. O. Omollo. Real time fraud detection system for mobile banking: Based on experiential paradigm, 2020.

[20] A. Phakatkar. Detection of credit card fraud using a hybrid ensemble model. *International Journal of Advanced Computer Science and Applications*, 13, October 2022.

[21] A. L. Prodromidis and S. Stolfo. Agent-based distributed learning applied to fraud detection. 1999.

[22] S. Sanober et al. An enhanced secure deep learning algorithm for fraud detection in wireless communication. *Wireless Communications and Mobile Computing*, 2021:e6079582, August 2021.

[23] TechTarget. What is ussd (unstructured supplementary service data)?, March 2024.

[24] M. Tehrani, Ali Asghar Amidian, J. Muhammadi, and H. Rabiee. A survey of system platforms for mobile payment. October 2010.

[25] B. William. Enhanced security model for mobile banking systems in tanzania. *International Journal of Technology Enhancements and Emerging Engineering Research*, 1:4–20, November 2013.