Development of a Fraud Alert System for Mobile Money Subscribers in Ghana

Owusu-Banahene Wiafe[1], Isaac Adjaye Aboagye[1*], Nii Longdon Sowah[1], Isaac Sai[1], Richard Osei Sakyi[1], Margaret Richardson Ansah[1], Percy Okae[1], Gifty Osei[1], and Edwin Okoampa Boadu[2]

[1]Department of Computer Engineering, University of Ghana, Legon, Accra, Ghana.

[2]Department of Biomedical Engineering, Koforidua Technical University, Faculty of Health and Sciences, Koforidua-Ghana

***Corresponding Author:** iaaboagye@ug.edu.gh

ABSTRACT

Mobile Money is a digital payment platform that allows for money transfers between mobile phone devices. Mobile money fraud has been rampant in recent years. Although the platform is secure, fraudsters can still find weaknesses in the gateway to defraud other mobile money subscribers. Currently, only the subscriber identification module (SIM) number or international mobile equipment identity (IMEI) that is used to commit fraud is blocked, which gives the fraudster the privilege to register and use a different SIM number. A mechanism is needed to block fraudsters permanently. In this study, we developed a system to alert mobile money users of fraudsters by screening incoming calls. We created a platform to help automate the registration of mobile money users using optical character recognition to obtain relevant information from an image of the user's ID card and a secure mobile application platform for mobile money transactions. Based on the information obtained, a mobile application was developed. Users were able to report a number that had attempted or succeeded in defrauding them. The mobile application has a broadcast receiver that listens to incoming calls or messages. The ID of the number making the incoming call is cross-checked with the caller ID stored in the telecommunication companies' database. When a fraudster is detected, subscribers will be alerted to allow the application to block that caller permanently. The system was tested to ensure its validity and performance. This system will help to reduce drastically the amount of money that mobile money subscribers lose.

Keywords: Mobile money, User ID, Fraudster, Subscriber, True caller application

1.0 INTRODUCTION

Mobile money service in Ghana is a technology that allows people to receive, store, and spend money using a mobile phone (World Remit, 2019). It is like opening an account with a bank but with more flexibility. For instance, you do not have to go to the automatic teller machine (ATM) or office to withdraw money. This can be done at any close mo-

-bile money vendor. Mobile money transactions are by far the backbone of daily trading in Ghana. According to the Bank of Ghana payment systems oversight annual report in 2020, mobile money transactions increased year-on-year by 42.27% in transactional volume from GH¢ 2 billion transactions in 2019 to GH¢ 2.86 billion in 2020. The total value of transactions also increased year-on-year by 82.37% from GH¢ 309.35 billion in 2019 to GH¢ 564.16 billion in 2020. It is not surprising that mobile users have already surpassed the number of people with bank accounts in Africa (Macharia, 2013).

In addition, banks have integrated mobile money into their systems to make banking more mobile and flexible. The mobile money platform is very promising, so people are now using it for malicious activities. One of the challenges that the mobile money platform faces right now is an increase in the number of fraudulent activities. Multiple reports of fraud via mobile money transactions have been made. Most target subscribers have less knowledge of how to prevent these activities. Fraudsters use different schemes to carry out these activities (Mabrie, 2015). This means that users will have to safeguard themselves against these fraudsters. Mobile money technology is very beneficial and essential to other nations in Africa. About 25% of Kenya's gross domestic product (GDP) flows through M-PESA, a mobile money platform in Kenya and the backbone of agriculture in Tanzania (Mugambi et al., 2014; Seetharam et al. 2015). Banking, insurance, healthcare, and other sectors in Africa are not excluded. Although the benefits are desired, the infiltration by fraudsters has caused so much financial loss to subscribers. This has damaged the reputation of the service and risks the industry as a whole (Sun et al., 2010). Many attempts have been made to reduce these fraudulent activities. Mobile money providers like M-PESA use AI to help deter fraudulent activities, but not all platforms use a similar approach (Zhdanova et al., 2014). It is also known that only 10% or less of fraud cases with mobile money are prosecuted by law (Ghanaweb, 2018). This means that the perpetrators of the act go scot-free. We developed a system to alert mobile money users of fraudsters by screening incoming calls in this research. It will also allow them to search and verify the number of perpetrators to prevent them from carrying out their scam activities. In addition, it is a mobile app that will serve as a secure platform for subscribers to carry out mobile money transactions. Mobile money service providers have tried their best to combat mobile money fraud over the past few years. Different algorithms have been performed to reduce fraud activities. Some of these existing systems and approaches have limitations that allow people to explore them. MTN Ghana has implemented a short message service (SMS) check that reads SMS sent via its network. This system checks the SMS content and blocks it from being sent if it has the same or similar structure as the official mobile money message received from legitimate money transfers. The system comprises a regular expression match layer to detect the structure of the message and a layer of artificial intelligence to detect

the context of the message and prevent it from being sent successfully. The limitation of this system is that it only checks for the SMS sequence for mobile money fraud activities.

In a true caller app, the data is crowd-sourced from the millions of users who have downloaded the true caller app on their smartphones. As part of the end-user agreement, the True Caller app asks the user to access the user's address book or contacts on the smartphone. The app then uploads this data to the company's servers (GitHub, 2020). This data collected is used to identify the names of new callers or message senders. Another feature of the true caller is that users can report numbers as spam numbers, and every user will be alerted of the status of that number (GitHub, 2020). The limitation of this system is that it is pervasive.

Isaac et al. did a qualitative study to explore the main causes of fraud in mobile money services in Ghana and the measures to combat the menace by the key stakeholders connected to mobile money services (Isaac et al., 2019). The study revealed that fraud in mobile money services is caused by weak internal controls and systems, a lack of sophisticated information technology tools to detect the menace, inadequate education and training, and the poor remuneration of employees. They proposed a detailed legal code and internal fraud policy to curb this menace. Their research did not propose an algorithm to reduce fraud activities.

Our proposed work involves a web application that implements a convolutional neural network for ID card classification during registration (Krizhevsky et al., 2017). Another layer extracts text data using optical character recognition and automatically fills the registration form. The ID information is linked with the user's data for easy tracking. All these are embedded in a web application that will allow telecommunication companies and users to blacklist fraudsters when identified. By using mobile broadcast receivers, incoming calls are screened to check for potential fraudsters. The mobile application uses data it receives from the web application to help prevent subscribers from these fraudsters. This research paper has been structured into five main sections. Section I is the introduction. It provides background information on the emergence of mobile money technology and how fraudsters have taken advantage of the technology to target users. In Section II, existing technologies for mobile money platforms are examined and reviewed to justify this research. Section III describes the system design and methodology of the proposed system. The hardware and software design are considered in this section too. Section IV focuses on the implementation and testing of the system to authenticate its functionality. It also analyses the results obtained from the tests and performance evaluation. Section V is the conclusion part of the paper. It highlights the key accomplishments of the work and possible recommendations for further work to enhance the performance of the system.

2.0 SYSTEM DESIGN AND METHODOLOGY

The system was designed to comprise two significant units, which are mobile application and web application. Figure 1 shows a high-level architecture of the system. The mobile application was built with Flutter allowing it to run on both IOS and Android devices. The functionalities specific to the native platform were developed in Java and Swift for Android and IOS, respectively. The mobile application serves as a means for subscribers to access the system. It communicates with the web application using the HTTP protocol over a RESTful API. The web application, on the other hand, was built with the PHP Laravel framework. It connects with a PostgreSQL database server to store data. It uses the Redis server for the caching of data. It also has a transaction processing monitor (TPM) script to connect to external databases for data queries. The web application provides a console and web interface for administrators to configure and manage the system. The system was designed to meet specific requirements. It was categorized into two main groups: functional and non-functional.

The functional requirement is to ensure that the system will allow the upload of images or snapshots from a camera, predict the type of ID card, extract text-relevant data from a photo of an ID card, link user data with the user's ID card, block a caller ID, report a fraud issue, and detect an incoming caller ID and provide the status. The non-functional requirement is to ensure that the system is usable, reliable, and web and Android-based. Figure 2 below illustrates the flow of information and how the mobile application works.

.

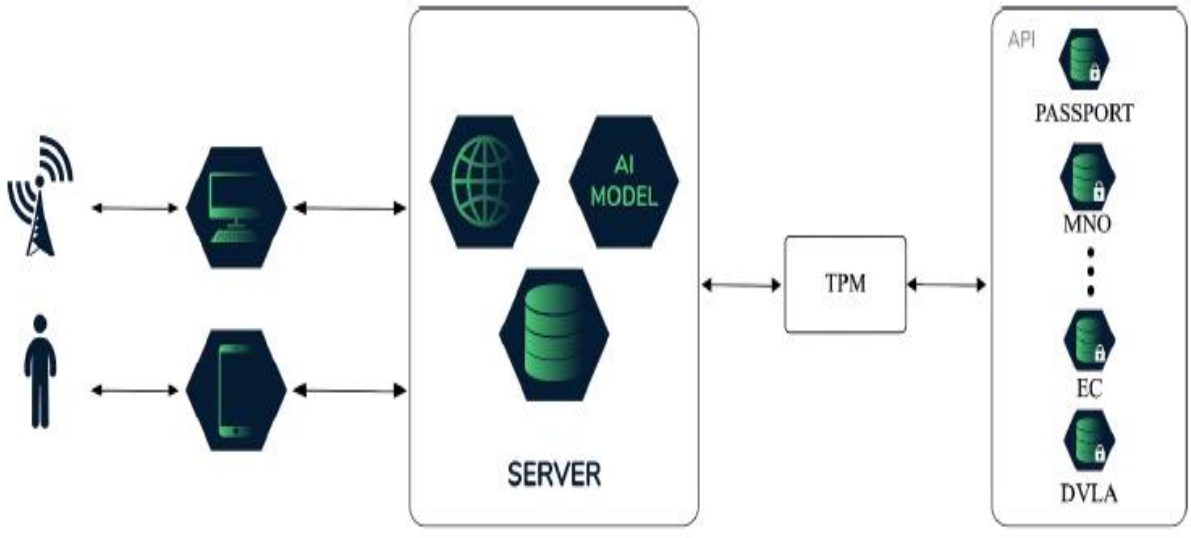

Figure 1: System Architecture

The mobile money subscriber can start using the application by registering. Without registering, they cannot proceed further with the use of the mobile application. After successful registration, they then log in to their account dashboard. At this stage, they can perform several actions like searching a number in the database, reporting fraud attempts, and blocking a fraudster's number. However, verifying incoming numbers from phone calls is automatically activated in the background as a service. Figure 3 shows the details of the number verification system. When a new call is detected using the native broadcast receivers, it starts a background service that makes an HTTP call with the incoming phone number to a REST endpoint on the web application. The number is searched for in the database. The user's status is displayed; otherwise, it tells the user that it cannot be found.

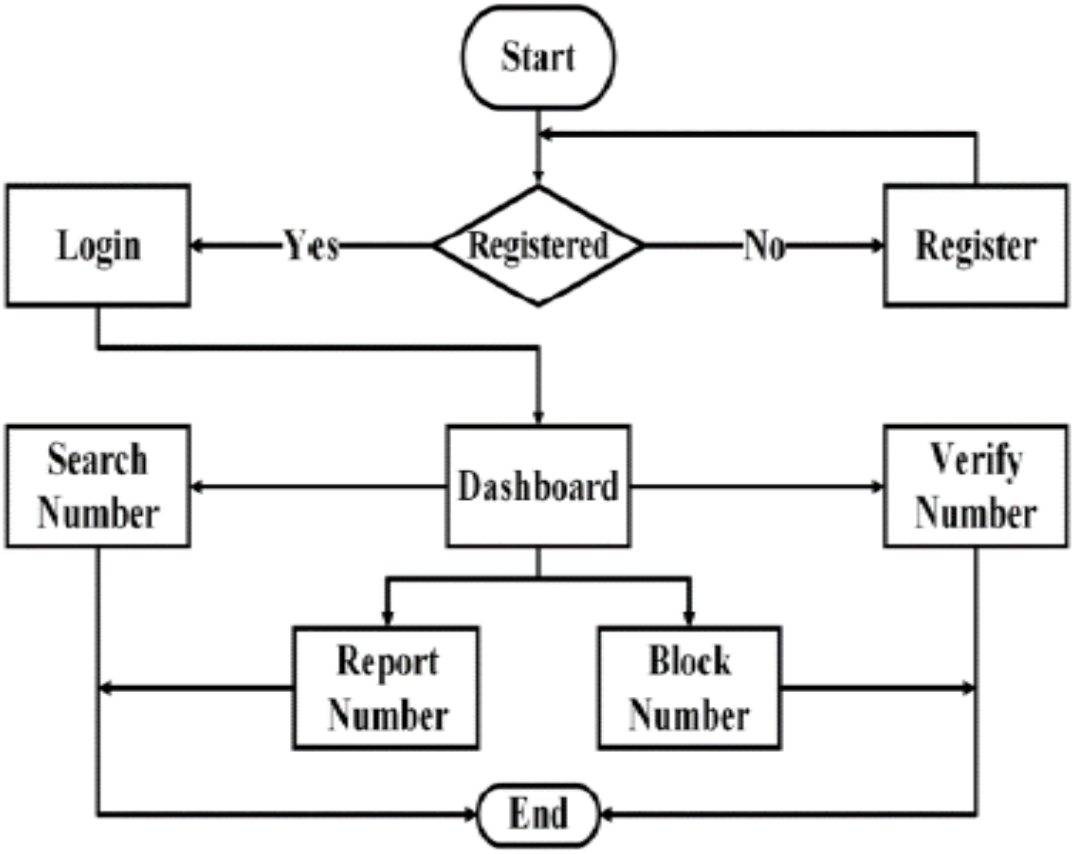

Figure 2: Flow Diagram for Registration

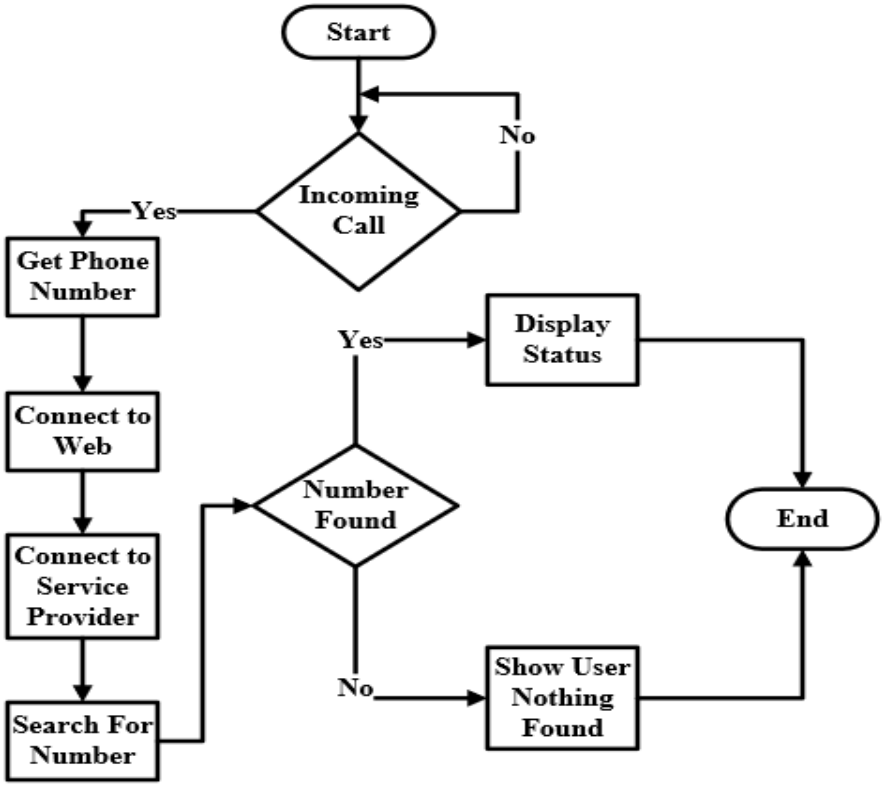

Figure 3: Flow Diagram for Incoming Call Verification

3.0 IMPLEMENTATION AND TESTING

The block diagram in Figure 4 shows the entire system and how the various components communicate. The web application lies in the center (Aboagye et al., 2012; Owusu-Banahene et al., 2021). It is connected to every component and serves as the master having the application logic. The subscriber's mobile application depends on the web application to make predictions, authenticate users, and perform other tasks that are not directly related to the device. The web application controls the creation, reading, updating, and deleting of data with the help of the PostgreSQL database. It also controls caching for authentication with the use of a Redis server. Figure 5 is a use-case diagram that represents the user's interaction with the system. It shows the relationship between the user and different use cases in which the user is involved. The registration, as shown in Figure 6, focused on ease of use to avoid user frustration. The name, email, and password are the details collected. Three input fields and a button are used to get the information. The data is sent to the web application using the HTTP protocol when the register button is pressed. The web application validates the data so that users cannot register multiple times with the same email. When the data is valid, it is saved in the database, and a JSON-created response with 201 status is returned. The mobile application shows a snack bar with a successful response or displays the error if any occurred.

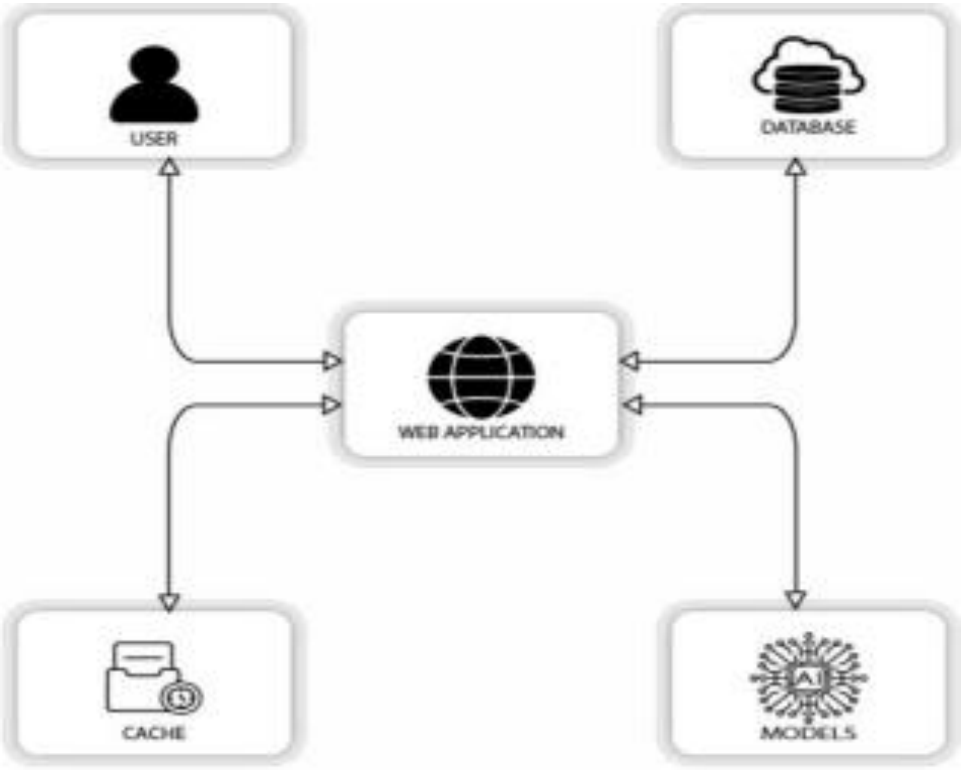

Figure 4: Block Diagram

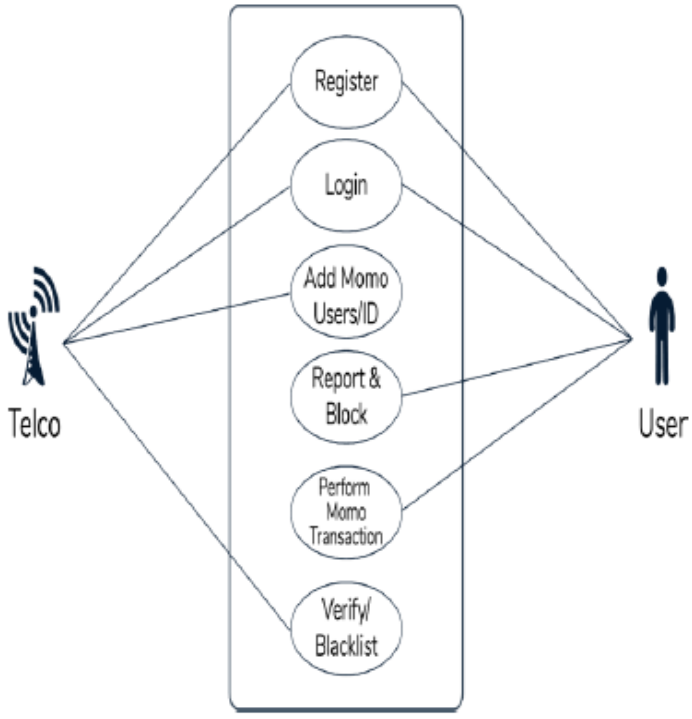

Figure 5: Use Case Diagram

To log in, only a unique email and password are required. Two input fields are provided with a button. When the button is pressed, the data in the field is validated for first-hand correctness before sending the request to the server using the HTTP protocol, as shown in Figures 7 and 8 below. Login may be accepted or denied. The server checks for the second-hand correctness of the data. When there is an error, it returns the error message with status 422. But when the user credentials are valid, a token is returned with the request with status 200. The mobile application displays the error if any, but when the authentication is successful, it saves the token in the application settings and navigates the user to the home page. In Figure 7, the Login was denied. Subscribers are provided with a quick but simple interface to make reports in the report lab.

They provide the fraudster's number and the reason or additional comments. After that, they press the report button. The data is then sent to the web applications to alert administrators to investigate and perform the necessary action quickly. The feedback of the report is shown to the user using a snack bar. Subscribers can quickly search for the status of a mobile money user in the search tab. This feature allows them to use the application to verify phone numbers they have received a call from on a different phone that does not have the application or help a friend or family. They are provided with an input

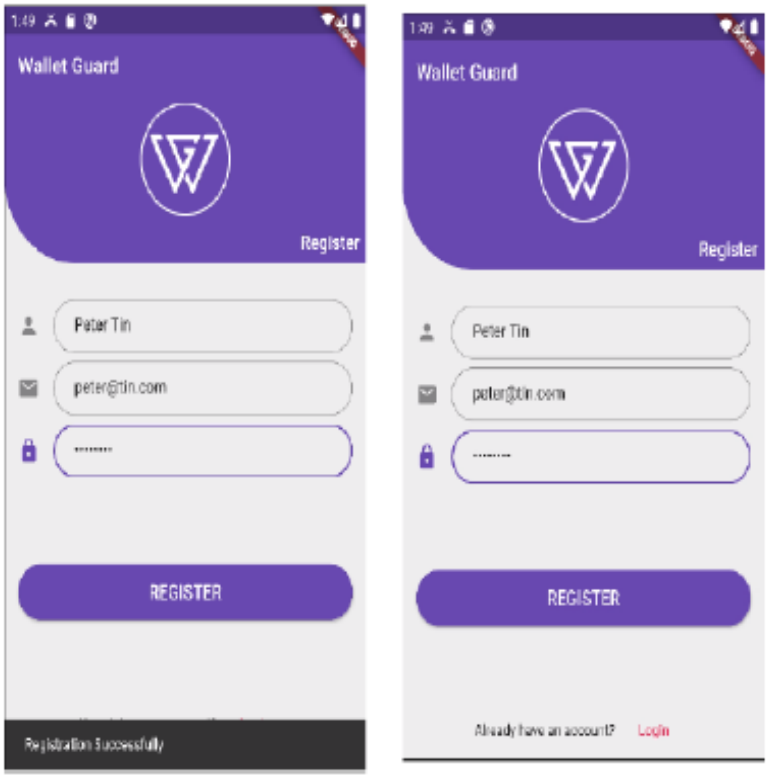

Figure 6: Subscriber Registration

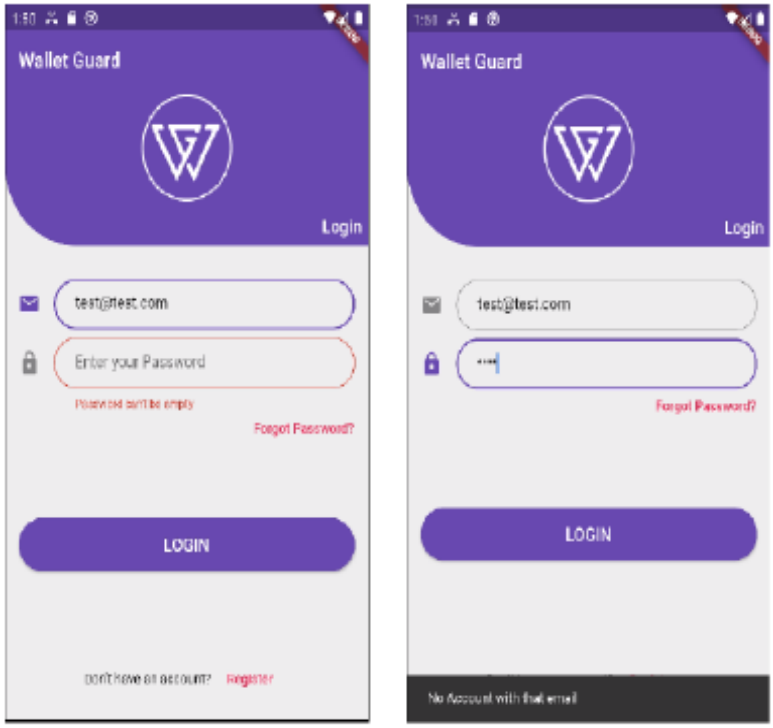

Figure 7: Login Denied

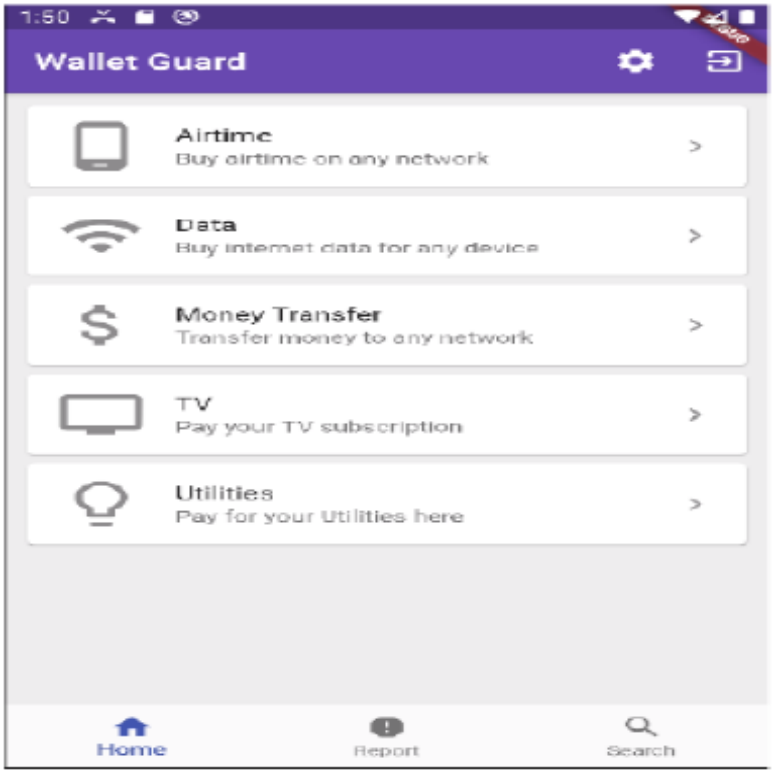

Figure 8: Login Successful

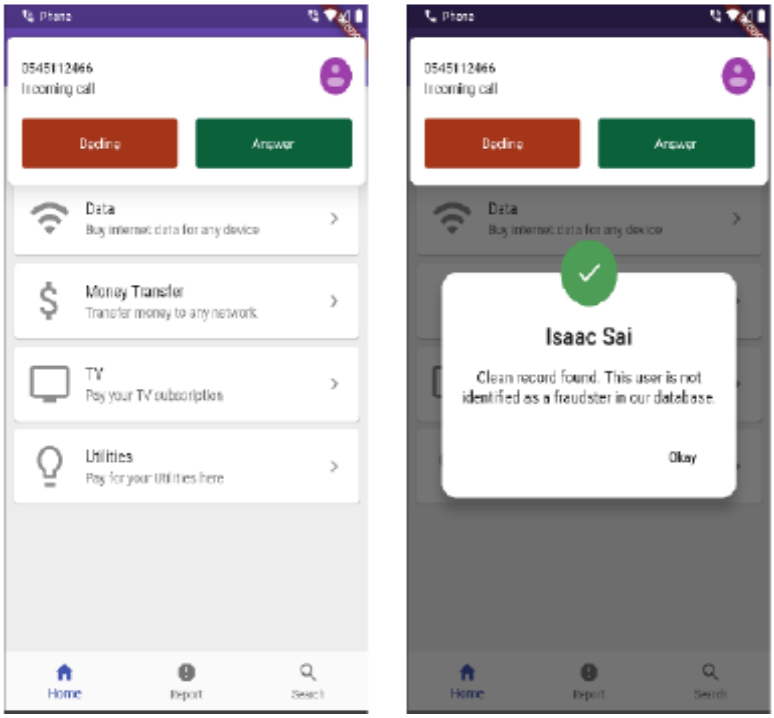

Figure 9: Legitimate Call Verification

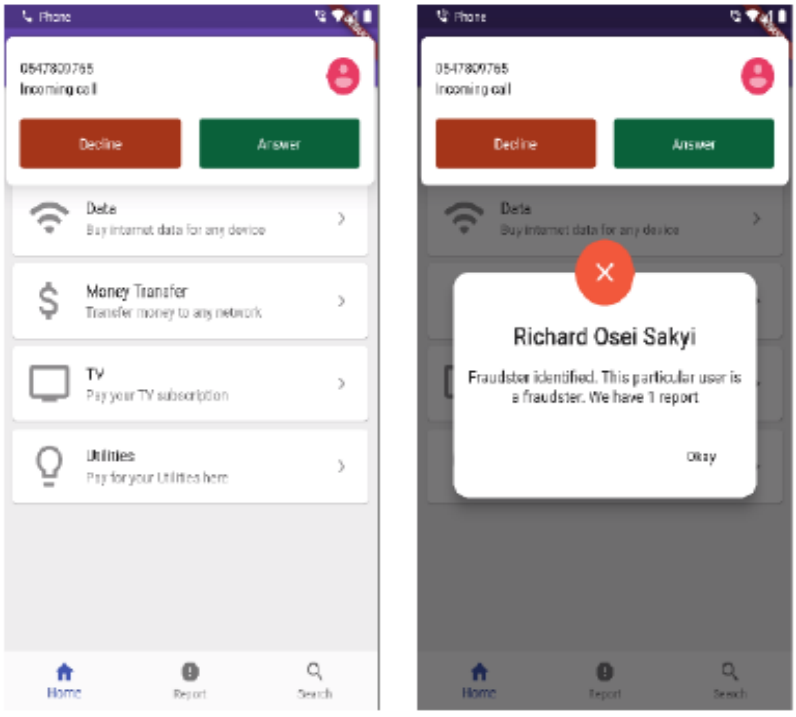

Figure 10: Fraud Call Verification

field and a search button. The number will be displayed after the mobile application requests the web application and receives the status. It is also possible for the application to do real-time number validation. When the subscriber logs in for the first time, a background service registers a broadcast receiver. This will enable the mobile application to know incoming calls and react to them. When an incoming call is deterred, an HTTP call is made to the web application with the phone number of the incoming call. The web application returns a JSON response indicating the status of the caller with reasons. The mobile application then displays it to the users to alert them. Figures 9 and 10 show legitimate call verification and fraud call verification, respectively.

4.0 CONCLUSION AND RECOMMENDATION

In our study, we developed a system to alert mobile money users of fraudsters by screening incoming calls. The system served as a common platform for multiple mobile money platforms to work effortlessly together. The main benefit the system provides is real-time communication between mobile money platforms and mobile money subscribers. Our system is an improvement on existing systems in terms of the design. This is because we introduced a transaction processing monitor which makes our system versatile in communicating with multiple databases at a time. This is an improvement on the work done by Isaac et al (2019). It also improves the pervasive nature of the true caller app and improves the SMS sequence check for mobile money fraud activities. Immediately a fraudster is identified and blocked, all the users of the system have access to that information which goes a long way to protect them and their wallets from fraudsters. From the results, the web application developed allows for all mobile money platforms to collaborate in fighting against fraud. It allows for the addition of any new mobile money platform. It also allows the platform to have one or more administrators to manage what happens. Furthermore, administrators can delegate registration tasks to registrars and ensure that reported cases are taken care of immediately. When mobile money users who have been reported are found to be guilty of the charges, they can be easily blocked, and all mobile money subscribers using the mobile application will be notified immediately. With the mobile application, mobile money subscribers can register and log in to the system on any mobile device having the mobile application installed on it. They can search for the status of a number to know whether it is safe to answer their call or reply to their messages. The added advantage is that when they receive incoming calls, the system automatically checks the caller's status before answering the call. This way, they are protected in advance. We recommend that an AI model should be integrated into the system. It will help to update the fraud database to the near real-time situation and make predictions by running the AI models in the background to retrieve the result and interpret it. Also, the Ghana card which contains the personal

information of the holder should be integrated into the system.

REFERENCES

World Remit. (2019). What is mobile money? Available: http://www.worldremit.com/en/mobile-money

Macharia, J. (2013). Mobile banking influence on wealth creation and poverty reduction for the unbanked. IST-Africa Conference and Exhibition, IST-Africa, 1–9.

Mabrie, B. (2015). The Wild West of Safeguarding Your Money: Mobile networks are at risk of being infiltrated by digital bandits. IEEE Consum. Electron. Mag., 4, 62–64.

Mugambi, A., Njunge, C., & Yang, S. C. (2014). Mobile-money benefits and usage: The case of M-PESA. IT Prof., 16(3), 16–21.

Seetharam, B., & Johnson, D. (2015). Mobile money's impact on Tanzanian agriculture. IEEE Software. 32(1), 29–34.

Sun, D., Pan, T., Wan, Z., & He H. (2010). Research of mobile commerce security solution based on an external electronic device. 6th International Conference on Semantics, Knowledge, and Grid, SKG, 355– 358.

Maria Z., Juergen R., Roland R., Chrystel G., & Baptiste H. (2014). No smurfs: Revealing fraud chains in mobile money transfers. 9th International Conference on Availability, Reliability, and Security, ARES, 11–20.

Ghanaweb. (2018). Mobile Money fraud: Only 10% of cases prosecuted due to the use of fake IDs. Available: https://www.ghanaweb.com/GhanaHomePage/busines s

GitHub. (2020). Git. Available: https://git-scm.com

GitHub. (2020). Build software better, together. Available: https://github.com.

Isaac, A. F., Charles A., & Agnes A. F. (2019). Control of fraud on mobile money services in Ghana: an exploratory study, 22(2), 300-317.

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. Commun. ACM, 60(6), 84–90.

Aboagye, I. A., Owusu-Banahene, W., Amexo, K., Boakye-Yiadom, K.A., Sowah, R.A., & Sowah, N. L., (2021). Design and Development of Computer Vision-Based Driver Fatigue Detection and Alert System, IEEE 8th International Conference on Adaptive Science and Technology (ICAST), Accra, Ghana, 2021, 1-6.

Owusu-Banahene, W., Aboagye, I. A., Boateng, F. F., & Boadu, A. A. (2021). Solid Waste Monitoring and Revenue Generation System, IEEE 8th International Conference on Adaptive Science and Technology (ICAST), Accra, Ghana, 2021, 1-6.