Mitigating Security Vulnerabilities in Offline USSD Payments in non-Smartphones: Enhancing User Privacy

MSc in Computer Science

Somtochukwu Anunobi

A025073m@student.staffs.ac.uk

Staffordshire University

A thesis submitted in partial fulfilment of the requirements of Staffordshire University for the degree of Master of Science in Computer Science (Software Engineering)

May 2024

Abstract

This study addresses security vulnerabilities inherent in traditional USSD peer-to-peer (P2P) transactions. These transactions, often relying on phone numbers or account numbers linked to digital wallets or bank accounts, expose users to social engineering attacks and lack protection against shoulder surfing due to the absence of masked PIN entry in USSD. To mitigate these risks, the study proposes a secure P2P system utilising unique wallet IDs and partial PIN entry. Validation tests confirm the effectiveness of the partial PIN method, reducing the probability of unauthorised access through shoulder surfing below 0.05%. User acceptance of unique wallet IDs is promising, with 78% of users favouring them for enhanced privacy and 82% expressing a desire to protect their personal information during transactions. Additionally, the study explores the voucher method as an alternative approach for P2P money transfers within the USSD framework. While the proposed system, including both partial PIN and unique wallet IDs, demonstrates significant security improvements compared to existing solutions, it does come at a cost. Transaction times increased by up to 88% for the proposed system and 101% for the voucher method. However, these increases remain within acceptable limits, staying between 22% and 70% below the 120-second USSD session duration threshold. Overall, this study highlights the effectiveness of the proposed security measures in safeguarding user privacy and enhancing transaction security in USSD P2P transactions, even with the observed increase in transaction time. These findings suggest a valuable trade-off between security and efficiency for promoting user trust and broader adoption of USSD-based financial services.

Keywords: **USSD, P2P Transactions, Mobile Payments, Security, Privacy, Social Engineering, Shoulder Surfing, Partial PIN, Unique Wallet ID, Voucher Generation, Mobile Money**

Acknowledgements

I want to begin by expressing my deepest gratitude to God for providing me with the strength and guidance to complete this project.

My heartfelt thanks go to my parents for their unwavering support and encouragement throughout this journey.

I am particularly grateful to my supervisor, Mehak Memon, for her invaluable guidance, mentorship, and dedication to reviewing my work. Her expertise and encouragement played a significant role in shaping this project into its final form.

I would also like to express my gratitude to my partner for her steadfast encouragement and care.

Finally, I extend my appreciation to all those who generously volunteered their time to test the implementation of this project.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

The rise of mobile phones has revolutionised financial transactions, with account ownership surging by 50% globally over the past decade (World Bank Group, 2021). This growth is particularly pronounced in developing economies, where mobile money has become a key driver of financial inclusion. In Sub-Saharan Africa, for example, a third of adults now hold a mobile money account (World Bank Group, 2021).

This surge in mobile financial inclusion can be attributed mainly to the rise of mobile wallets. These versatile applications offer a convenient and secure alternative to traditional methods like cash or cheques. They allow users to store and use payment information, pay bills, and conduct peer-to-peer (P2P) transactions directly from their mobile devices (Ramli & Hamzah, 2021; Kumar et al., 2017). Notably, mobile wallets bridge the gap for those lacking reliable internet access. Unlike internet-dependent mobile banking solutions, many mobile wallets can leverage Unstructured Supplementary Service Data (USSD) – a technology that utilises existing mobile network infrastructure – to facilitate transactions even on basic feature phones.

This empowers individuals in underserved communities who might otherwise be excluded from the digital financial revolution to participate in the financial ecosystem. Financial institutions have embraced these mobile payment technologies, recognising their potential to expand their reach and connect with a broader audience, including those without internet access.

For regions lacking reliable internet access, Unstructured Supplementary Service Data (USSD) has emerged as a powerful tool. Defined by (European Telecommunications Standards Institute, 1997), USSD, also known as quick codes or feature codes, is a communication protocol that allows GSM phones to interact directly with mobile network

operators (MNOs). Unlike SMS, USSD is a real-time session technology that is a versatile tool for offline mobile applications, particularly in the areas of banking services, data collection, messaging, and information access (Lakshmi et al., 2017; Perrier et al., 2015), making it possible for basic feature phones to engage in the digital financial ecosystem. USSD has been particularly impactful in developing economies, particularly Sub-Saharan Africa, where it plays a crucial role in driving financial inclusion (Neza & Joseph, 2022).

1.1 Motivation

However, despite USSD's role in expanding financial inclusion, existing approaches using USSD for banking services, particularly in the context of offline P2P payments with non-smartphones, face several security challenges regarding user privacy risks and authentication.

Privacy is defined as the individual's ability to control what personal information is disclosed, to whom, when, and under what circumstances (Song et al., 2018). Personal information, according to the General Data Protection Regulation (GDPR) in Article 4(1), refers to any information that relates to an identified or identifiable natural person (eds. O. Radley-Gardner et al., 2016).

Authentication is the process of verifying a user's identity before granting access to a system. It acts as a security checkpoint, ensuring only authorised individuals can enter (Vinay Kumar B, 2022).

USSD peer-to-peer transactions typically require personal information like phone numbers, as most USSD digital wallets are tied to the user's phone number as a primary identifier (Perrier et al., 2016; Mallik et al., 2020; Hussaini et al., 2020; Dayang & Hamza, 2021). These identifiers, while convenient, pose a significant threat to user anonymity. Since these identifiers are likely used by users across various systems, including those unrelated to

payments, sharing them during USSD transactions exposes users to potential identification risks in these other systems.

For instance, a user might share their phone number for a USSD-based P2P transaction. If the recipient utilises the same phone number to identify the user on another platform (social media, for example), the user's anonymity within the P2P transaction is compromised. This can have privacy implications and potentially lead to targeted scams or social engineering attacks (Lakshmi et al., 2017; Binitie et al., 2021).

Unlike other applications, such as browsers and mobile apps that utilise PIN-masking features, Unstructured Supplementary Service Data (USSD) relies solely on plain text entry. This inherent characteristic eliminates functionalities like hidden PIN fields, rendering user input during a USSD session susceptible to observation. Consequently, USSD transactions are vulnerable to shoulder surfing attacks, where a malicious actor can easily steal sensitive information (e.g., PINs and account numbers) by observing a user's keypad entries during a USSD session (Binbeshr et al., 2021).

These vulnerabilities expose users to potential risks, such as data breaches and unauthorised access to their financial information.

This research delves into this critical gap in USSD security. We aim to identify existing vulnerabilities and propose innovative solutions that safeguard user privacy and strengthen authentication mechanisms in offline P2P transactions facilitated by USSD technology. By addressing these security challenges, we can ensure a more secure and trustworthy USSD experience, empowering individuals to participate fully in the digital financial ecosystem.

1.2 Aim

To develop and evaluate a user-friendly offline USSD payment system with a focus on enhancing user privacy and security.

1.3 Objectives

1. To investigate the current utilisation of USSD for payment transactions.
2. To assess the security implications associated with existing USSD-based payment models.
3. To design a secure offline P2P payment system via USSD that utilises strong customer authentication while preserving user anonymity for basic feature phones.
4. To evaluate the proposed USSD P2P system against existing solutions based on user experience, security, and speed.

1.4 Deliverables

1. Literature review on existing research on Unstructured Supplementary Service Data (USSD) payment systems.
2. Critical analysis of USSD Usage for payment systems, identifying strengths and possible research gaps.
3. Development and deployment of a prototype showcasing the proposed enhancements to USSD-based payment systems.
4. A comparative evaluation assessing the security, speed and user experience of the implementation prototype against existing solutions.

2 Literature Review

2.1 Introduction

The review examines the current state of research on Unstructured Supplementary Service Data (USSD) technology, specifically focusing on its use in peer-to-peer (P2P) financial transactions. It explores the potential security risks and user privacy risks associated with USSD-based P2P transactions.

This literature review delves into the existing research surrounding USSD with a particular focus on its application for peer-to-peer transactions. It explores the user privacy risks and security challenges posed by USSD, and reviews strategies proposed to mitigate these challenges. The review is structured first to outline the foundational theories and principles of USSD, followed by an examination of the difficulties inherent in USSD peer-to-peer transactions.

Furthermore, the review will analyse various approaches that have been proposed or implemented to mitigate these security challenges, identifying the research gap.

2.2 USSD Technology

USSD (Unstructured Supplementary Service Data) is a technology built into the GSM standard, the most common standard for mobile networks globally (Nyamtiga et al., 2013). This inherent advantage makes USSD universally available on all GSM mobile phones, encompassing both sophisticated smartphones and basic phones with limited functionalities. These basic phones, often referred to as "feature phones," lack the advanced capabilities of smartphones but can still leverage USSD for various purposes.

2.3 USSD Architecture

USSD (Unstructured Supplementary Service Data) functionality is detailed in US Patent No. US5752188A (1994) (Bo A. V. Äström & Björn A. Svennesson, 1998). The patent outlines a system wherein the Mobile Network Operator (MNO) establishes a Service Code (SC) for user access to USSD services.

2.3.1 Network Infrastructure

The network infrastructure of USSD, as depicted in Figure 2.1, is composed of various components.

Service Code Dialling: The user initiates a USSD session by dialling a specific service code on their mobile phone and pressing "Send."

Signalling Channel Transmission: The network interprets the dialled code as a USSD code and transmits it, along with any associated data, via a dedicated signalling channel.

Mobile Switching Centre (MSC): The data reaches the Mobile Switching Centre (MSC), a central network element responsible for call routing and handover.

Lookup Process: At the MSC, a lookup process is initiated. The Visitor Location Register (VLR) is consulted first to determine the user's current network location.

Home Location Register (HLR): If the code is not recognised within the VLR, a subsequent lookup is performed against the Home Location Register (HLR)—the HLR stores subscriber-specific information, potentially including pre-defined USSD services associated with the user's account.

USSD Application: Upon successful identification of the code, the USSD application residing within the MSC executes the corresponding action(s). This often involves initiating a menu-driven interaction that presents the user with various options.

External Network Nodes (Optional): An essential aspect of USSD's dynamism lies in the ability of the handler to direct requests. It can leverage pre-defined services stored in the HLR or route them to external network nodes, such as gateways dedicated to USSD-based applications (e.g., USSD banking).

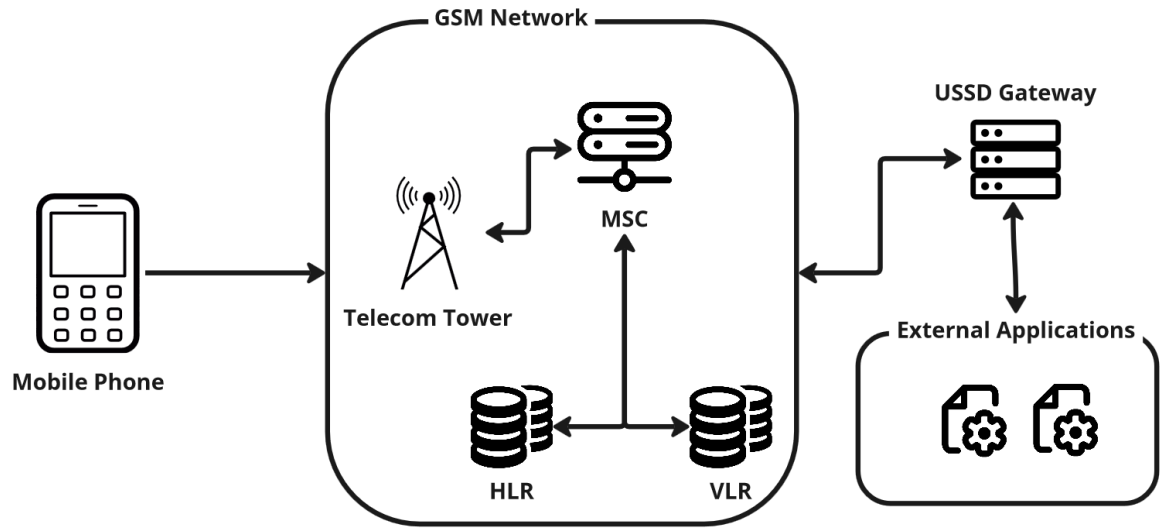

Figure 2.1 USSD System Architecture

The arrows in Figure 2.1 indicate the direction of data flow. When a USSD session is initiated from the mobile phone, the request travels through the GSM network to the USSD Gateway. The Gateway then communicates with the relevant external application to process the request and deliver a response back to the user's phone. The HLR and VLR databases are queried during this process to ensure proper routing and authorisation.

2.3.2 User Interaction with USSD

A USSD session provides a unique user experience distinct from traditional mobile applications. It employs a text-based interface, where navigation unfolds through a series of menus and prompts rather than graphical elements.

Initiation: The user dials a specific service code on their mobile phone and presses "Send."

Connection and Response: The network establishes a connection with the USSD application. Depending on the code's validity and user eligibility, the user receives either an initial response or an error message.

Menu Navigation (Optional): If the code is valid, a menu is often presented with numbered options representing distinct functionalities. The user selects an option by entering the corresponding number and sending it back to the USSD session.

Textual Input (Optional): In some instances, the user might be required to provide textual input, such as account details or personal information.

Dynamic Interaction: Prompts and responses adapt based on user choices and input, creating a dynamic interaction within the session.

Session Progression: The user journeys through a series of prompts and responses, effectively defining a structured flow for the session. This back-and-forth exchange continues until the user accomplishes the intended task, reaches a final message, or elects to terminate the session actively.

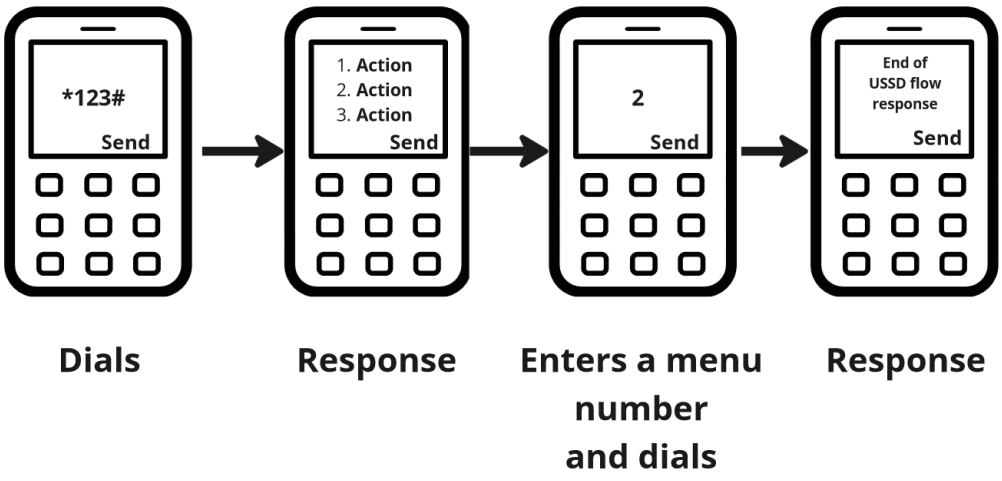

Figure 2.2 USSD flow for a user.

Figure 2.2 exemplifies the initial USSD menu (represented by the *123# code and options 1-3) displayed on the phone screen. The user interacts with this menu by entering a number corresponding to the desired action (represented by the arrow pointing to option 1). This selection triggers the USSD system to send a request to the relevant application and subsequently displays a new menu or response based on the user's choice. This iterative process of menu navigation and user response selection continues until the user completes their task, receives a final message, or chooses to end the session.

2.4 Related Works

(Mallik et al., 2020) They proposed a USSD-based digital wallet system aiming to consolidate various financial functionalities for users with basic feature phones. This system leverages an open-source API to facilitate bill payments, merchant transactions, peer-to-peer transfers, and more, all through USSD menus. Existing digital wallet users authenticate with a PIN, eliminating additional verification steps since the phone number is inherently linked to the USSD session. A user-friendly menu guides users through available services like bill payments or money transfers. For instance, paying car insurance involves selecting the insurance company, entering the policy number, and initiating payment or viewing details.

While comprehensive, this USSD digital wallet solution raises security concerns requiring further exploration. First, the system's sole reliance on PIN-based authentication presents a significant vulnerability. Weak PINs are susceptible to brute-force attacks and unauthorised observation (shoulder surfing), potentially leading to compromised accounts and fraudulent transactions. Implementing more robust authentication methods, such as multi-factor authentication (MFA), is recommended to enhance user account security significantly.

Second, the use of phone numbers for transactions raises user data confidentiality concerns. Sharing phone numbers exposes sensitive user data, potentially leading to unauthorised

access or account takeover. Further research is necessary to explore and implement methods that either anonymise transactions or minimise data exposure within USSD-based digital wallets. This proactive approach is crucial to safeguard user privacy and ensure the integrity of the entire digital wallet ecosystem. Addressing these security concerns can pave the way for a more robust and trustworthy USSD digital wallet platform.

(Mallik et al., 2020) The digital wallet approach offers convenience for basic phones, but security weaknesses remain. PIN-based authentication is vulnerable, and phone numbers expose user data.

(Hussaini et al., 2020) They proposed a USSD-based cashless revenue collection system designed to streamline transactions and payments using mobile phones. The system is managed by a task force, often contracted by state or local government authorities, which may employ agents such as payment point officers, admins, and checkpoint officers to manage payment terminals, validate transactions, and top up users' digital wallets. The task force utilises a desktop version of the system for tasks like generating real-time revenue reports, registering users, creating checkpoints and enrolment points, and topping up digital wallets. On the other hand, motorists, the primary users, utilise the mobile version of the system to make revenue payments, check balances, and top-up their digital wallets using USSD commands.

The system proposed offers a significant contribution by facilitating remittance for the informal sector. By providing a streamlined and accessible cashless revenue collection system, the proposed solution empowers individuals in the informal sector to participate in digital transactions without relying on traditional cash-based methods or needing internet access or smartphones. This democratisation of financial services not only enhances convenience for users but also fosters financial inclusion by extending the benefits of digital

payments to a broader segment of the population. However, a significant security concern arises from the system's reliance on USSD for user authentication, which employs a PIN. This method presents a vulnerability, as unauthorised individuals gaining access to both the mobile phone and PIN could potentially make payments on behalf of the user. This highlights the need for more robust authentication mechanisms to safeguard against unauthorised access and ensure the security of transactions conducted via USSD.

(Hussaini et al., 2020) The approach offers cashless payments and financial inclusion for the unbanked (basic phones) with a focus on remittances. Still, it relies on weak PIN authentication, highlighting the need for more robust security measures.

(Binitie et al., 2021) Investigate the security challenges of USSD transactions in the context of financial services. They acknowledge the widespread adoption of USSD due to its accessibility on basic feature phones. However, they identify a critical security concern: the vulnerability to shoulder surfing attacks. Since USSD displays sensitive information like PINs in plain text, bystanders can easily steal this credential. Their research highlights a fundamental limitation – existing secure authentication methods often rely on non-textual data formats like images or colours, which are incompatible with the text-based nature of USSD. This incompatibility explains the continued prevalence of PIN-based authentication in USSD transactions despite the existence of potentially stronger alternatives.

(Binitie et al., 2021) Acknowledges USSD's role in financial inclusion for basic phones but raises security concerns due to its text-based nature, leaving PINs vulnerable to shoulder surfing.

(Dayang & Hamza, 2021) Propose a USSD-based mobile payment system that caters to offline transactions on basic feature phones. This system offers a valuable solution by enabling offline payments even with limited functionalities. Here, the customer shares their

phone number with the seller, who then initiates a USSD query with the customer's number and transaction amount. A secure platform interacts with the customer via SMS for confirmation and sends a validation code. The customer enters this code alongside a secret code to verify the transaction. Upon confirmation, the platform debits the customer's account and sends success messages to both parties. Finally, the seller completes the transaction by paying the customer.

While this approach offers convenience for basic phones, it's essential to consider user privacy within the USSD framework. Sharing phone numbers during the transaction exposes user data. Additionally, if someone gains access to a customer's phone number and the USSD code, they could potentially initiate fraudulent transactions. This observation highlights the ongoing challenge of balancing user convenience with robust security measures in USSD-based systems, particularly regarding user data confidentiality and unauthorised access prevention.

(Dayang & Hamza, 2021) Propose secure offline USSD payments for basic phones through USSD and SMS verification, but user data is exposed through phone number sharing needed to conduct the transactions. This highlights the ongoing challenge of balancing convenience with user privacy in USSD.

(Patience et al., 2022) proposed a system named "transcare," which introduces a multi-layered security approach for transaction authentication. The system utilises a one-time-PIN (OTP) mechanism, automatically generated at the conclusion of each transaction and delivered to the user's registered mobile phone via Short Messaging Service (SMS). These OTPs remain valid until usage and are required before granting access to any services. Additionally, the system employs a Bag of Soft Biometrics (BOSB) feature, consisting of security questions registered by the user during the initial setup. These questions are

presented randomly to the user during each transaction, ensuring that only the user knows the answers. This multi-layered approach enhances security by mitigating the risk associated with device compromise, as knowledge of the user's device alone is insufficient to conduct transactions. Furthermore, each new transaction prompts a different set of security questions from the BOSB. By requiring OTP validation for each transaction and presenting randomised BOSB questions, the system ensures that even if an individual gains access to a user's device, they would still be unable to conduct transactions without knowledge of the OTP and BOSB answers.

Implementing similar security measures in USSD peer-to-peer payment systems can significantly enhance their security posture. By integrating OTP validation and BOSB authentication, USSD payment systems can effectively mitigate the risk of unauthorised access and fraudulent transactions. However, it is essential to note that while these security measures enhance transaction security, they do not address concerns regarding user confidentiality.

(Patience et al., 2022) The approach uses a multi-layered approach of SMS and security questions to secure USSD transactions, mitigating unauthorised access even if the user’s device is compromised. However, this approach does not address privacy leakage concerns present in USSD peer-to-peer transactions.

(Wycliffe Ochieng’ Agwanyanjaba, 2020) Proposed a system incorporating USSD push notifications as an additional security measure for transactions, aiming to enhance transaction security by requiring users to validate transactions through their registered phone number and device. Upon registration on the platform, users' phone numbers are linked to their unique phone ID (IMEI), ensuring that USSD push notifications are only sent to authorised devices.

The utilisation of USSD push notifications represents a significant advancement in transaction security, as it adds an extra layer of confirmation, thereby ensuring that the transaction request originates from the application installed in the user's authorised device. This approach provides users with greater confidence in the security of their transactions, helping to mitigate the risk of unauthorised access and fraudulent activities.

However, it is essential to acknowledge the inherent limitations of USSD technology. USSD operates as a single-channel communication protocol, allowing only one USSD session at a time. As a result, integrating USSD push notifications into the transaction process may pose challenges, particularly if the user concurrently initiates other USSD-based operations. The restriction to a single USSD window for user input may potentially hinder the effectiveness of USSD push notifications in improving transaction security.

(Wycliffe Ochieng' Agwanyanjaba, 2020) Proposes USSD push notifications for two-factor authentication, but it excludes all basic phones and doesn't address user data privacy concerns.

(Njuguna Michael, 2020) Suggested enhancing the security of USSD transactions by implementing security questions, where users are required to provide answers they know during the transaction process. This additional layer of security aims to mitigate the risk of unauthorised access in scenarios where another individual gains physical access to the user's phone and device. However, while security questions add a level of authentication, they remain vulnerable to shoulder-surfing attacks.

Despite providing an additional barrier to unauthorised access, participants still have to share identifiable information to conduct transactions, hence making it susceptible to privacy leaks and social engineering attacks.

(Njuguna Michael, 2020) The approach of an additional security layer asking a security question adds an extra layer of security to PIN authentication but is still vulnerable to user data privacy leaks.

(Olamilekan et al., 2022) They proposed a USSD-based system that enables users to create digital vouchers and convert them into their digital wallets, mainly focusing on airtime vouchers of various denominations. Telecom companies generate these vouchers, which can be converted into e-cash through the USSD platform. The system also offers the option to rectify erroneous transactions. To initiate transactions, users are required to input a PIN for authentication. Once authenticated, the system identifies the banks associated with the user's phone number, allowing them to select the desired account for the conversion of airtime to e-cash.

One of the critical contributions of this system is its ability to address the needs of individuals who may not have access to traditional banking services or reliable Internet connectivity. By allowing users to convert airtime vouchers into e-cash via USSD, the system extends financial services to underserved populations, promoting greater financial inclusion and empowerment. This novel method offers an alternative means of depositing funds, thereby reducing barriers to entry and expanding access to digital financial services.

While this approach ensures user confidentiality by eliminating the need to share personal details between users, it introduces security vulnerabilities. For instance, if a voucher intended for one user is obtained by another user or observed by a third party, it can be loaded into their account, leading to unauthorised transactions. Moreover, the lack of multifactor authentication (MFA) in the USSD system poses a security risk.

(Olamilekan et al., 2022) The approach promotes financial inclusion for the unbanked by enabling voucher conversion to USSD digital wallets. Still, it raises security concerns due to weak authentication and the potential for unauthorised voucher use.

2.5 Critical Analysis

Table 2.1 Critical Analysis Summary

Title	Author	Year	Key points	Observations
USSD Digital Wallet	Mallik et al.	2020	• Proposes a USSD-based digital wallet system for basic feature phones. • Leverages an open-source API to facilitate various financial services like bill payments, money transfers, e-shopping, etc. • Uses PIN code for user authentication (existing digital wallet users). • Offers a main menu for selecting specific transactions.	• PIN-only authentication creates a security risk: ○ Vulnerable to unauthorised access if PIN is compromised. It highlights the need for stronger authentication, like multi-factor authentication, for USSD-based digital wallets.

			Pro: The digital wallet approach offers convenience for basic phones **Con:** Prone to brute force attacks, shoulder surfing and user privacy leaks	

A USSD-Based Cashless Revenue Collection System: Targeting the Informal Sector	Hussaini et al.	2020	• Proposes a USSD-based cashless revenue collection system for mobile payments.
			• System managed by the task force (government contracted) with agents (payment officers, admins, checkpoint officers).
			• Taskforce uses desktop versions for reports, user registration, checkpoint creation, and digital wallet top-ups.
				• Contribution
				  ○ Facilitates remittance for the informal sector.
				  ○ Enables cashless transactions without internet or smartphones.
				  ○ Promotes financial inclusion for a broader population.
				• Security concern
				  ○ PIN-based USSD authentication is vulnerable.

			• Motorists (users) use mobile versions for payments, balance checks, and USSD top-ups. **Pro:** An excellent adaptation of using USSD for peer-to-peer remittances targeted at the informal sector. **Con:** Prone to brute force attacks, shoulder surfing and privacy leaks.	○ Unauthorized access to phone and PIN allows fraudulent payments. • Need for more robust authentication mechanisms for USSD transactions.
Implementing Existing Authentication Models in USSD Channel	Binitie et al.	2021	• Analyses security challenges in USSD-based mobile banking transactions. • Highlights vulnerability to shoulder surfing attacks due to plain text display of PINs.	• Standard PIN entry method remains prevalent in USSD due to challenges in implementing more robust alternatives.

			• Points out limitations of existing secure authentication methods (non-textual data) for USSD. **Pro:** USSD is widely accessible on basic phones, promoting financial inclusion. **Con:** Vulnerability to shoulder surfing attacks due to plain text PIN display, incompatibility with more robust non-textual authentication methods and user privacy leaks.	
Using USSD-based Mobile Payment in the Context of Low Internet Connection	Dayang and Hamza	2021	• Proposes a USSD-based mobile payment system for offline transactions with basic phones. • Customer provides a phone number to the seller.	• Convenient solution for basic phones but with security concerns: ○ Sharing phone numbers exposes customer details.

			• Seller initiates USSD query with a customer number and amount to a secure platform. • Platform interacts with customers via SMS for confirmation and a validation code. • Customer enters code and secret code to confirm. • Platform debits customers, sends success messages, and the seller completes the transaction. **Pro:** Enables secure offline payments on basic phones through USSD and SMS verification.	○ Vulnerable to unauthorised access through phone number. • Highlights the need for more secure USSD systems for user privacy and preventing unauthorised access.

			Con: Privacy leakage through phone number sharing for transactions.	

Security against Shoulder Surfing Attack Adaptable to Feature Phones using USSD Technology.	Patience et al.	2022	• Uses One-Time PIN (OTP) via SMS for transaction authentication (valid until used).
			• Employs Bag of Soft Biometrics (BOSB) with user-registered security questions.
			• Presents random BOSB questions during transactions for additional verification.
			Pro: Introduces a multi-layered security approach (OTP + BOSB) for USSD transactions.
			Con: While strengthening transaction security, this approach doesn't address
				• Contribution
				  ○ Significantly enhances security by mitigating risks from device compromise.
				  ○ OTP and BOSB make unauthorised transactions difficult.
				• Security concerns
				  ○ User confidentiality remains a concern.
				• Further improvements are needed to safeguard user data privacy.

			privacy leakage concerns present in USSD systems.	

Enhanced Mobile Banking Security: Implementing Transaction Authorization Mechanism Via USSD Push.	Wycliffe Ochieng' Agwanyanjaba	2020	• Proposes USSD push notifications as an additional security measure for USSD transactions.
			• Users validate transactions via phone number and device (linked to IMEI during registration)
			Pro: Push notifications are used as a two-factor authentication for USSD transactions.
			Con: Excludes all basic feature phones.
				• Contribution
				  ○ Additional security layer through USSD-push notifications.
				  ○ Requires confirmation from the authorised device for transactions.
				  ○ Increases user confidence in transaction security.
				• Limitations concerns
				  ○ Can only work with a smartphone that is able to install the mobile application.

				• Integrating push notifications might be challenging with concurrent USSD operations since only one USSD input window can be opened at a time.

Dynamic Knowledge-Based Authentication Model for Enhancing Security of USSD Banking Transactions	Njuguna Michael	2020	• Proposes security questions for additional security in USSD transactions.
			• Users answer pre-registered questions during transactions.
			Pro: Introduces an additional security layer (security questions) for USSD transactions.
			Con: While strengthening transaction security, this approach doesn't address
				• Contribution
				  ○ Adds an extra layer of authentication.
				  ○ Mitigates risk of unauthorised access if someone has the user's phone.
				• Security concerns
				• Vulnerable to shoulder surfing attacks if someone observes the user entering answers.

			privacy leakage concerns present in USSD systems.	

Dynamic Knowledge-Based Authentication Model for Enhancing Security of USSD Banking Transactions	Njuguna Michael	2020	• Proposes security questions for additional security in USSD transactions.
			• Users answer pre-registered questions during transactions.
			Pro: Introduces an additional security layer (security questions) for USSD transactions.
			Con: While strengthening transaction security, this approach doesn't address privacy leakage concerns present in USSD systems.
				• Contribution
				  ○ Adds an extra layer of authentication.
				  ○ Mitigates risk of unauthorised access if someone has the user's phone.
				• Security concerns
				• Vulnerable to shoulder surfing attacks if someone observes the user entering answers.

Design and Simulation of	Olamilekan et al.	2022	• Proposes a USSD system to create and convert airtime	• Contribution

Unstructured Supplementary Service Data (USSD) to Fund Bank Accounts using Mobile Recharge Credit Vouchers			vouchers to e-cash in digital wallets (focuses on airtime vouchers). • Vouchers from telecom companies are converted through the USSD platform. • Offers error correction for transactions. • PIN-based authentication protects confidentiality (users don't share personal details). **Pro:** Provides financial inclusion and access to digital services (voucher conversion to e-cash) for the unbanked or those without internet via USSD.	○ Addresses needs of unbanked/unconnected populations. ○ Extends financial services for financial inclusion. ○ Offers an alternative for depositing funds and accessing digital financial services. • Security concerns ○ Vouchers are vulnerable to unauthorised use if obtained by others. ○ Lack of multi-factor authentication (MFA) creates a security risk.

			Con: Introduces new security concerns - unauthorised voucher use if obtained/observed and lack of strong authentication (MFA) beyond PINs in the USSD system.	• PIN alone may not be sufficient to prevent unauthorised transactions.

The critical analysis of existing research on USSD-based mobile payments reveals valuable insights into security strengths and weaknesses. By identifying limitations in current approaches, such as reliance on weak PINs and user data confidentiality concerns, this study paves the way for the development of a more robust and secure USSD-based P2P transaction system.

2.6 Research Gap

Several studies have explored the use of USSD for financial transactions (Owusu et al., 2018; Mallik et al., 2020). However, security concerns have been raised due to USSD's limitations in authentication and user data confidentiality (Lakshmi et al., 2017; Otor et al., 2020). These limitations stem from USSD's reliance on text-based communication, making it challenging to implement robust security measures.

2.6.1 User Privacy Risks

The use of phone numbers as identifiers poses significant privacy and security risks, including unwanted exposure and harassment (McDonald et al., 2021)

USSD wallets designed for peer-to-peer (P2P) transactions often rely on phone numbers as unique identifiers, requiring them to be shared with other participants during the transaction (Dayang & Hamza, 2021; Mallik et al., 2020).

When users engage in USSD transactions, their phone numbers essentially become the key to their financial interactions. This reliance on phone numbers as unique identifiers means that they must be shared with other participants during transactions, particularly in P2P transactions facilitated through USSD wallets.

Under regulations such as the EU's General Data Protection Regulation (GDPR), phone numbers are considered identifiable user data (Cormack, 2020, 2021). The sharing of phone

numbers within USSD transactions extends beyond the transactional framework, potentially exposing users to risks outside of their immediate transactional context. This data can be exploited in various ways, including targeted social engineering attacks, where malicious actors manipulate individuals into divulging sensitive information or performing actions that compromise their security (Njuguna Michael, 2020).

Furthermore, the susceptibility to social engineering attacks is heightened by the widespread use of phone numbers as identifiers across various digital platforms and services. Once a phone number is compromised through a USSD transaction or any other means, it can serve as a gateway for attackers to launch coordinated attacks, access additional personal information or even gain unauthorised access to accounts linked to that number (Bullée et al., 2016).

While USSD transactions offer convenience and accessibility, the reliance on phone numbers as identifiers raises significant concerns regarding user data confidentiality and privacy.

A gap exists in exploring methods that balance user identification for security purposes with anonymity features to protect user privacy during P2P transactions. There is a need for innovative approaches that conceal user data during USSD transactions while ensuring robust security against unauthorised access and fraudulent activities.

2.6.2 Limited Authentication

Studies by (Lamoyero & Fajana, 2023) highlight the weak authentication methods used in USSD transactions, with some requiring only a single PIN and others lacking any authentication altogether. This vulnerability is further underscored by (Binitie et al., 2021), who discuss various robust authentication techniques like image, colour, and biometric verification that enhance security for transactions on other channels like mobile apps. However, these methods require functionalities beyond essential text input, making them

incompatible with USSD's text-based nature. Consequently, USSD remains reliant on PINs, which are susceptible to brute-force attacks (repeatedly guessing the PIN) (Vugdelija et al., 2021) and shoulder surfing (observing someone entering their PIN) as users' input is not masked during entry (Binbeshr et al., 2021).

While USSD (Unstructured Supplementary Service Data) offers a lifeline for mobile banking and financial services in regions with limited internet and smartphone penetration, its inherent limitations create security vulnerabilities. The key challenge lies in developing stronger authentication methods that are resistant to these attacks while remaining compatible with the limitations of basic phone interfaces.

2.6.3 Limited Exploration of Alternative P2P USSD Payment Approaches

Existing research on USSD-based P2P transactions primarily focuses on replicating existing mobile payment models within the limitations of USSD technology. A gap exists in exploring alternative approaches specifically designed for peer-to-peer payments using USSD.

The research gaps provide specific areas for further investigation, all aiming to address the inherent limitations of USSD while enhancing security and user privacy, especially for P2P transactions and primary feature phone users.

In summary, the identified research gaps are:

- User Privacy Risks: Sharing phone numbers as identifiers exposes users to social engineering attacks due to GDPR and widespread phone number usage across platforms.
- Limited Authentication: PIN-based authentication is vulnerable to brute-force attacks and shoulder surfing due to the lack of masked input in USSD's text-based format. Existing robust methods like biometrics are incompatible with USSD.

- Limited Exploration of P2P Approaches: Research focuses on replicating existing mobile payment models within USSD limitations, neglecting exploration of alternative P2P-specific approaches.

Mitigation Strategies:

- Develop methods that balance user identification for security with anonymity features to protect privacy during P2P transactions (e.g., one-time tokens).
- Design stronger authentication methods compatible with basic phone interfaces and user literacy, potentially using alternative approaches beyond PINs.
- Explore alternative P2P USSD payment approaches specifically designed for the limitations and functionalities of USSD technology.

3 Research Methodology

3.1 Introduction

Research methodology refers to the systematic and logical plan used to investigate a research question (Bairagi & Munot, 2019). It involves various methods like experimentation, observation, analysis, comparison, and reasoning to arrive at sound conclusions.

This chapter details the research methodology used to address the limitations identified in USSD-based transactions, particularly those related to user data confidentiality and weak authentication in peer-to-peer (P2P) payments facilitated through USSD wallets.

3.2 Research Design

This study aimed to design and prototype a secure and user-friendly USSD digital wallet system. This system utilises a unique combination of knowledge-based authentication (KBA) and PIN authentication. Our objective was to address the critical gap in user data confidentiality and strengthen authentication mechanisms within USSD-based P2P payments, specifically for users of basic feature phones. To achieve this, we employed a pragmatic research approach**.** A practical approach, as highlighted by (Clarke & Visser, 2018), provides researchers with the flexibility to hire a range of strategies, enabling a deeper understanding of the impact of methodological choices, making it particularly well-suited for technology-focused research where the goal is to develop practical solutions to real-world problems (Baltes & Ralph, 2021).

3.3 Unique One-Time Wallet Identifiers

The proposed system addressed the identified user privacy leak associated with phone number sharing during P2P transactions in section 2.6.2 by introducing unique, one-time-use

wallet IDs generated by the recipient. This eliminated the need for the recipient to share their phone number, significantly enhancing user confidentiality.

Previously, a typical P2P transaction flow involved sharing user phone numbers, as shown in Figure 3.1, exposing user data and raising privacy concerns. This system addressed this issue by allowing the recipient to proactively generate a unique wallet ID specifically for receiving a single payment, as shown in Figure 3.2. This ID, valid for a limited time, replaced the phone number during the transaction. By adopting this approach, the system ensured that user phone numbers remained confidential throughout the P2P process.

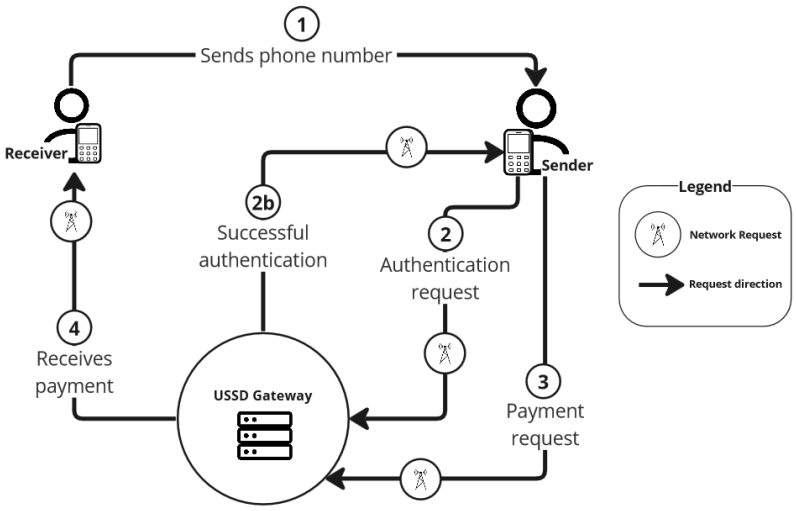

Figure 3.1 USSD peer-to-peer transaction flow with phone numbers in existing implementations.

Figure 3.1 depicts the user interaction with the USSD digital wallet while performing a peer-to-peer transaction using the sharing of identifiable information. This exposes the user's phone number and raises concerns about privacy risks.

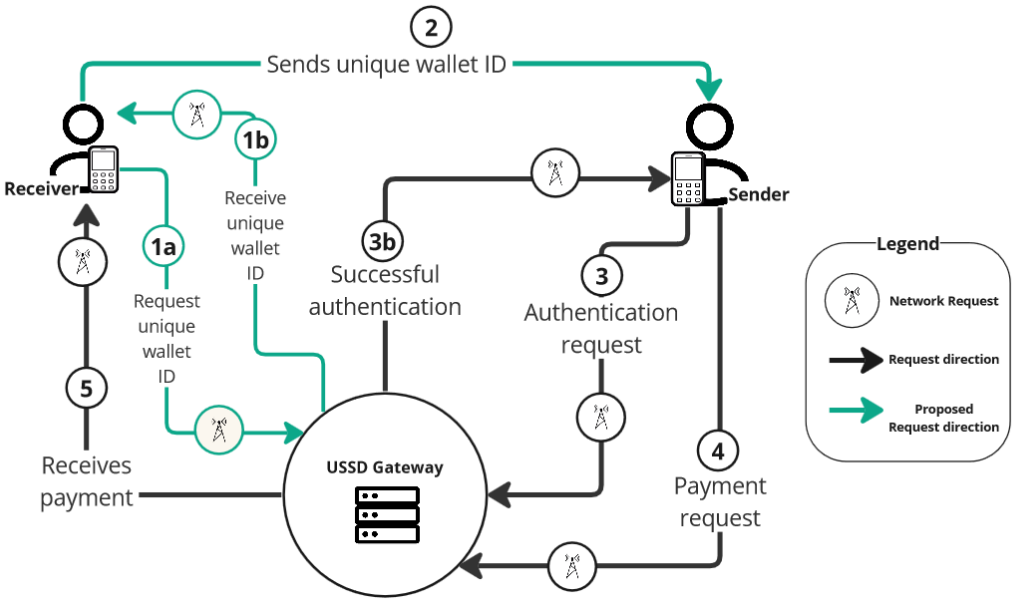

Figure 3.2 USSD peer-to-peer transaction flow with unique wallet Identifiers in proposed implementation.

Figure 3.2 depicts the user interaction with the USSD digital wallet while performing a peer-to-peer transaction with the additional layer that uses unique wallet IDs instead of personally identifiable information.

3.4 Partial PIN Challenge

The implemented system utilised a partial PIN challenge for user authentication, addressing the limited authentication gaps in USSD peer-to-peer transactions in section 2.6.2. This method replaced the standard approach of requiring the entire PIN during login attempts. In the proposed approach, users were prompted to provide three characters from their PIN, but the positions of these characters were randomised each time. The user's PIN itself was derived from information they already knew (Jakobsson & Liu, 2013). This approach required users to respond to a provided challenge by deriving and entering a response based on their original PIN and the received challenge. This resulted in a unique response for each login session, minimising the risk of shoulder surfing and recording attacks (Binbeshr et al.,

2023). Compared to the standard method of requiring the entire PIN every time, the random subset PIN challenge verification added an extra layer of security. Even if an attacker observed the user entering digits during a login attempt, they wouldn't be able to directly determine the complete PIN due to the constantly changing requested positions.

According to (Sheil & Malone, 2022), there is a moderate chance of recovering a full PIN from partial entries with persistent guessing (tens to hundreds of attempts). The system employs safeguards to prevent this. It implements a limit on unsuccessful attempts. After exceeding this limit, the system defaults to Multi-Factor Authentication (MFA) in section 3.5. This ensures the full PIN remains secure even against brute-force attacks.

3.4.1 Secure PIN Storage

To ensure a higher level of security, the system avoids storing the user's PIN in plain text within the database. This critical step prevents unauthorised access to user credentials even in the event of a database breach. The next chapter delves into the details of a specific cryptographic algorithm employed by the system to achieve this secure PIN storage. This algorithm allows the system to verify the user's response during the random subset challenge without ever needing to access or store the PIN in plain text.

3.4.2 How it Works

- **User enters a PIN (during registration):** During registration, the user creates a secret PIN, which serves as the basis for authentication. This PIN must be between 6 and 8 digits long. For example, 654321.
- **Login attempt:** The user attempts to log in.
- **System generates a challenge:** The system randomly selects three positions from the PIN (e.g., positions 1, 2, and 4).

- **System presents a question:** The system asks the user to enter the digits at the specified positions. In this example, the question might be: "Enter the 1st, 2nd, and 4th digits of your PIN."
- **User responds:** The user, knowing their PIN, enters the digits at the requested positions (in this case, they would enter "653").
- **System verifies:** The system retrieves the stored complete PIN (654321) and extracts the digits corresponding to the requested positions (which is also "653"). If the extracted digits match the user's response, the system grants access. Otherwise, access is denied.
- **Login attempts:** The system locks out the user on three failed attempts and defaults to the multi-factor authentication method to reset the trials.

3.5 Multi-factor Authentication with Bag of Soft Biometrics

To address the limitations of single-factor PIN authentication identified in section 2.6.2, this system implements multi-factor authentication (MFA) as an additional security layer. MFA is mandatory for high-risk transactions exceeding 50,000 Naira or to reset failed PIN challenge attempts.

The system leverages a Bag of Soft Biometrics (BoSB) approach for MFA. As described by (Nandakumar & Jain, 2009), soft biometrics refer to behavioural or personality characteristics

that offer some user identification information but are insufficient for definitive identity verification.

By requiring answers to randomly chosen security questions during registration, the system ensures that each user has a unique set of questions. This approach makes it more challenging for attackers posing as legitimate users to gain access, even if they register on the platform.

3.5.1 How it Works

- **User answers questions (during registration):** During registration, the system randomly selects three distinct questions from the pre-defined pool for the user to provide answers to.
- **MFA Activation:** In scenarios requiring MFA:
    - For high-value transactions exceeding 50,000 Naira, alongside the PIN challenge, the user is required to answer one randomly chosen question from the three distinct questions they answered during registration.
    - For PIN trial resets, the system prompts the user to answer one (not necessarily all three) of the pre-defined security questions. Answering correctly allows the user to reset their PIN and regain access to their account.

3.6 Secure Vouchers for Enhanced Flexibility

To address the limitations identified in section 2.6.3, this system introduces secure vouchers for peer-to-peer (P2P) transactions, which are particularly useful in remittance scenarios, as illustrated in Figure 3.3. These vouchers offer increased flexibility and convenience, complementing the unique wallet ID approach.

3.6.1 How it Works

- **Voucher generation**: The user generates a voucher with the chosen denomination for an intended user using the recipient's unique wallet ID.
- **Sharing Vouchers:** Once generated, users share the voucher details with the recipient.
- **Voucher Redemption:** The recipient uses the received voucher details to redeem the specified amount within the system. Importantly, each voucher can only be redeemed once and only by the intended recipient. This single-use nature, combined with not requiring the recipient's phone number, significantly enhances security against unauthorised access and shoulder surfing attempts.

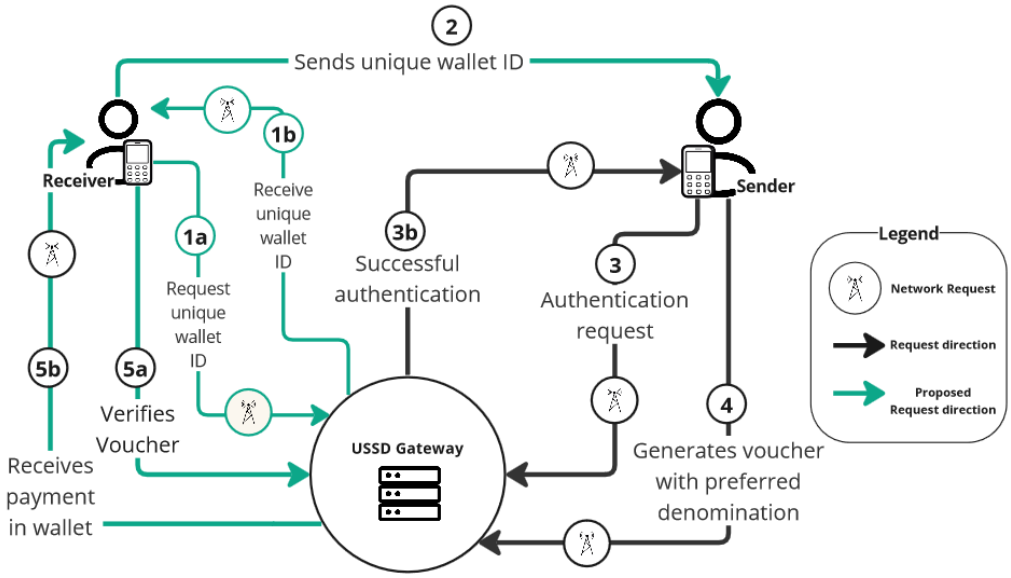

Figure 3.3 Flow for Generating and Redeeming Secure Vouchers

3.7 Data Collection

Data collection encompasses a range of techniques and tools used in research to gather and process data systematically (Sukmawati, 2023). The research employed two primary techniques:

3.7.1 USSD Session Logs

Logs captured directly from the USSD service itself provided valuable insights into session durations and the number of "hops" (data exchanges) that occurred during USSD communication. Logs were collected from both the sandbox environment and real user devices interacting with the USSD application. Analysing these sessions and hops allowed for a comparative assessment of the proposed approach with existing methods in terms of average speed and user experience.

3.7.2 User Experience Survey

Participants who used the USSD platform on their devices were invited to complete a questionnaire designed to gather their insights and experiences. The questions focused on user patterns and overall impressions of the system, providing valuable qualitative data.

3.8 Existing Implementation for Comparison

To ensure an accurate comparison, a replica of an existing USSD digital wallet system was created (Somtochukwu Anunobi, 2024). This implementation incorporated the following limitations commonly found in existing systems, which the proposed solution aimed to address:

1. Weak Authentication: Existing systems often display the user's PIN in full view during input, posing a security risk. To address this, the implemented replica required users to enter their PIN digits one at a time, masking the input for enhanced security.
2. User Privacy Leaks: Many existing implementations require phone numbers for money transfers, potentially compromising user privacy. The replica addressed this by not requiring phone numbers for transactions.

By creating a comparable existing implementation, a more targeted evaluation of the proposed solution's benefits could be conducted.

3.9 Location of Study

USSD service codes are typically assigned by Mobile Network Operators (MNOs) and vary depending on the region. Due to limitations in time and resources, this study utilised two service codes:

3.9.1 Real-World Testing

A service code assigned by African Talking (Africa's Talking, 2024), accessible to all Nigerian MNOs, was used for real-life testing with user devices. This selection reflects Nigeria's well-developed banking ecosystem, considered to be one of the most advanced in Africa. It is important to note that while only accessible within Nigeria, roaming Nigerian numbers were able to access it globally.

3.9.2 Simulation Testing

A separate service code, not tied to any specific MNO, was used for simulation-based testing within a controlled sandbox environment. This allowed for testing independent of geographical location.

3.10 Data Generation

A USSD digital wallet typically collects customer data like full names and phone numbers during registration (Mallik et al., 2020). However, to prioritise participant privacy in this study, a different approach was taken for real-world testing. Participants did not have access to each other's phone numbers, as this aligned with the study's objectives.

To avoid the need for actual money transactions, each user received a random amount of virtual currency credited to their USSD wallet upon registration. These virtual units allowed participants to complete the assigned tasks within the system.

For the simulation-based testing conducted in a controlled environment, dummy data was generated using database seeding techniques within the Adonis JavaScript framework (Adonis JS Lucid, 2024).

3.11 Data Analysis

Data analysis is the process that involves evaluating data using analytical and logical reasoning, and it can be used to extract useful information for business decision-making (Islam, 2020).

This analysis focused on three critical aspects of the USSD digital wallet system: security, speed, and user experience. Security assessments ensured the system's effectiveness in protecting user data. Speed analysis evaluated the efficiency of transactions within the USSD framework. Finally, user experience analysis aimed to understand participants' ease of use and overall satisfaction with the system.

3.12 User Testing

For the user testing phase, a group of twenty participants was recruited to test the USSD digital wallet system in real-world situations. These participants were chosen using a convenience sampling method, a common approach in research where readily available individuals are selected (Emerson, 2021). All participants in this study had prior experience using USSD banking applications and had access to a Nigerian phone number, ensuring a basic level of familiarity with the technology. Each participant was tasked with completing a series of actions using the system to evaluate its usability and effectiveness.

3.12.1 Telegram for Privacy

Telegram messaging application (Telegram, 2024) was chosen as the platform due to its focus on privacy. Unlike traditional messaging apps where phone numbers are visible. Telegram

allows users to interact using usernames, mimicking the real-world scenario where senders wouldn't necessarily know the recipient's phone number when using the USSD wallet for money transfers.

To facilitate the testing process:

- **Supergroup with Subgroups**: A supergroup was created within Telegram, containing subgroups for each user. Each subgroup held the specific tasks assigned to a participant. This structure ensured clear organisation and individual instructions.
- **Telegram Bot Automation:** A custom Telegram bot was programmed to automate several tasks:
- **Task Tracking:** The bot assigned each user random Letters as their names, kept track of their progress and assigned tasks, ensuring everyone completed the necessary actions.
- **Matching Recipients:** Based on the assigned letters, the bot anonymously matched participants for money transfers, simulating real-world scenarios without revealing phone numbers.

The test users were divided into two groups of ten. This allowed for the evaluation of potential performance variations. One group tested the applications during the daytime, while the other tested at night. This aimed to assess the impact of time of day on performance and user experience. Each user received a random amount of virtual currency upon registration in their USSD wallet. This eliminated the need for actual money transactions while allowing users to complete the assigned money transfer tasks.

3.13 Performance Measurement with USSD Session Logs

To compare the performance of the existing and proposed USSD implementations, logs were collected from Africa Talking. These logs captured the duration of each session (request and response).

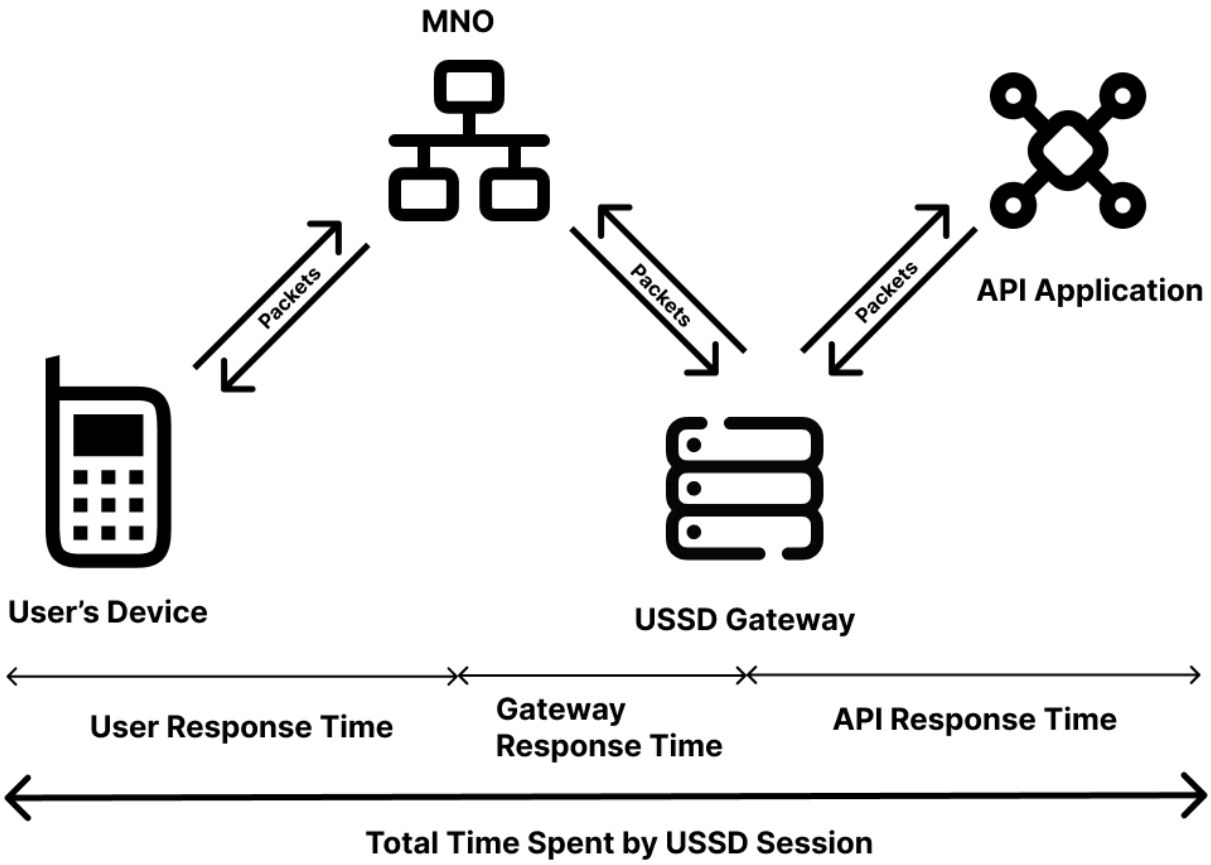

Figure 3.4 USSD Session Duration

On average, the total time duration of USSD sessions in Nigeria lasts approximately 120 seconds (Wavinya, 2024). The USSD session logs represent the combined response times from various elements:

User Response Time: This refers to how long it takes you to interact with a service offered on your phone through a USSD menu (like entering numbers to check your balance). This

includes the time spent reading the menu options, understanding them and entering responses. This is between 30 and 50 seconds for Nigerian Telcos (Wavinya, 2024).

Gateway Response Time: The time it takes for the USSD gateway to receive and respond to packets from the MNO.

API Response Time: The time it takes for the API to send and respond to packets from the USSD gateway.

By analysing these logs, we could assess:

Comparison of Implementations Overall Speed: The average time taken to complete transactions within each implementation. This was crucial in understanding how the proposed solution impacted speed and user experience compared to the existing system.

Time-of-Day Impact: Whether there were any significant differences in performance between daytime and nighttime testing.

3.14 Design Phase

The research leverages Computer-Aided Software Engineering (CASE) tools. Draw.io was utilised to produce high-level design documents. These documents included use cases, entity relationship diagrams (ERDs), sequence diagrams, and class diagrams.

3.15 Prototype Development Methodology

To handle the unique challenges and time constraints of a USSD prototype, Agile development with Test-Driven Development (TDD) was chosen. This iterative approach (Kumar & Sowmyavani, 2012) ensured continuous testing and code improvement, which is crucial for a successful USSD solution.

3.16 Development Tools

The system utilised a MySQL database to securely store user information, transaction data, and unique wallet IDs. Redis database for session caching. JavaScript, chosen for its vast open-source library ecosystem, served as the primary programming language, enabling efficient development and integration of essential functionalities for the USSD digital wallet. A USSD Simulator from (Africa’s Talking, 2024b) was employed to test the USSD application's endpoints thoroughly.

3.17 Summary

The research employed a pragmatic research approach with a combination of simulation-based testing and real-world user testing in Nigeria. Convenience sampling was used to recruit participants who evaluated the system's usability and effectiveness through a user experience survey and session Logs.

4 Design of Artefact

4.1 Requirement Analysis

Requirement analysis is a critical step in designing a secure and user-friendly USSD P2P transaction system (Grady, 2007). This analysis focuses on addressing essential shortcomings in the security and user privacy leaks in USSD peer-to-peer transactions, raising some key questions: How can we enhance user privacy in USSD peer-to-peer transactions? How can the system mitigate over-the-shoulder attacks, especially considering PINs are entered in plain text? Can alternative transaction methods beyond immediate money transfers be explored?

The solution introduces several measures:

- Unique One-Time Wallet IDs: Replacing static identifiers with unique IDs protects user privacy during transactions.
- Partial PIN Entry: Users would only enter a portion of their PIN during login and transactions, reducing the risk of someone observing the complete PIN.
- Flexible Transactions: Users will have the option to generate vouchers with specific denominations that others can redeem, offering an alternative to direct transfers.

The following sections will detail the functional and non-functional requirements identified based on this analysis.

4.1.1 Functional Requirements

- User Management
    - Users should be able to register for the system by creating a PIN and answering security questions.
    - Users should be able to log in using a random subset of their PIN.

    - Users should be able to reset their PIN using multi-factor authentication (MFA) with Bag of Soft Biometrics (BoSB).
- Peer to peer Transaction
    - Users should be able to initiate P2P transactions by specifying the recipient's unique wallet ID and the amount to be sent.
    - The system should allow the receipt of money to USSD digital wallets via a generated wallet ID.
    - The wallet IDs should be valid for only one transaction within a specified time duration.
    - The system should allow for secure voucher generation with chosen denominations for P2P transactions.
    - Users should be able to share voucher details with intended recipients through any communication channel.
    - Recipients should be able to redeem vouchers using the received details within the system. Each voucher should be single-use and only redeemable by the intended recipient.
- Security
    - The system should generate unique, one-time-use wallet IDs for recipients to eliminate the need for sharing phone numbers during P2P transactions.
    - The system should not store user PINs in plain text. A secure cryptographic algorithm should be used for PIN storage.
    - The system should limit unsuccessful login trials to prevent brute-force attacks.
    - The system should implement multi-factor authentication (MFA) for high-risk transactions and PIN reset attempts.

    - MFA should leverage BoSB, requiring users to answer randomly chosen security questions from a pre-defined pool.
- Additional functionalities
    - The system should display clear USSD menus and prompts to guide users through transactions.
    - The system should provide transaction history and balance inquiries.

4.1.2 Non-Functional Requirements

These requirements describe desirable system attributes and serve as constraints on how the system was to be designed. They were

- Performance
    - The system should respond to user inputs and requests promptly to ensure a seamless user experience.
    - Transaction processing times should be fast and meet user expectations, especially for critical actions like money transfers.
- Availability
    - The USSD service should be highly available with minimal downtime to ensure users can access their accounts and perform transactions reliably.
- Security
    - The system should employ robust security measures to protect user data and financial information from unauthorised access, theft, or manipulation.
    - The system should comply with relevant data privacy regulations (e.g., GDPR) regarding user data collection, storage, and usage.
- Usability

    - The USSD interface should be user-friendly and intuitive, catering to users with varying levels of technical literacy.
    - The system should provide clear instructions and error messages to guide users through the process.
- Scalability
    - The system should be scalable to accommodate a growing user base and transaction volume without compromising performance or stability.
- Interoperability
    - The system should be interoperable with other relevant financial services or platforms to facilitate broader adoption and financial inclusion.

4.2 System Architecture

4.2.1 Data Layer

At the foundation lies the data layer, which houses a secure database. An in-memory database (IMDB), Redis and a relational database management system (RDBMS), MySQL. The Redis is used for caching and session management. At the same time, the MySQL database is responsible for storing critical user information, including hashed PINs (to prevent plain text storage), unique wallet IDs for P2P transactions, and transaction history that excludes recipient details to maintain user privacy. Additionally, the MySQL database stores details of generated vouchers, such as their denomination, unique identifier, recipient's wallet ID, and redemption status.

4.2.2 Application Layer: Core Functionalities and Security

Building upon the data layer is the application layer. This layer acts as the heart of the system, handling the core functionalities that users rely on. It encompasses user registration, login processes, P2P transactions (including voucher generation and redemption), and

account management. The application layer implements the business rules and logic that govern these operations, ensuring everything runs smoothly. Notably, a subset of the application layer is dedicated to security. This security layer employs a cryptographic hashing algorithm, such as SHA-256, to store user PINs securely. This one-way encryption process safeguards user credentials even in the event of a database breach.

4.2.3 Communication Layer

The communication layer acts as a bridge, connecting the user interface with the core system. A key component within this layer is the USSD Gateway. This gateway facilitates the exchange of USSD messages between the user's mobile phone and the application layer. It plays a crucial role in ensuring reliable communication by parsing requests and responses into formats that both the user's phone and the system can understand.

4.2.4 Presentation Layer

At the very top of the system architecture sits the user interface, represented by the USSD menu. This menu provides a user-friendly interface for interacting with the system. It displays clear options and guides users through transactions intuitively.

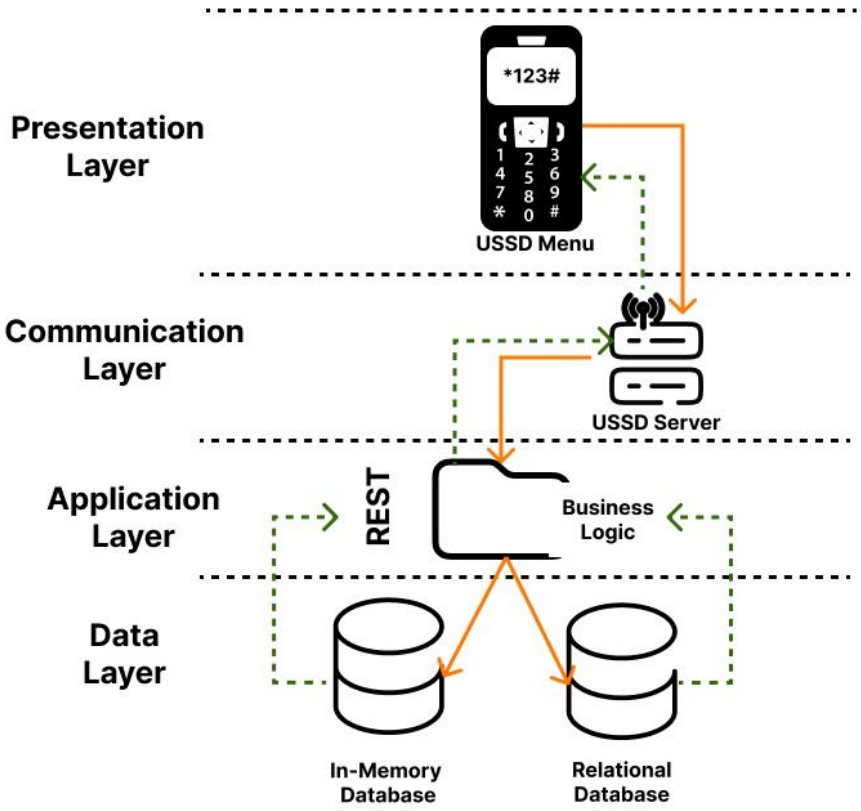

Figure 4.1 Application System Architecture

4.3 System Design

This section delves into the system design of the application leveraging a combination of Unified Modelling Language (UML) diagrams

4.3.1 Wire Frames

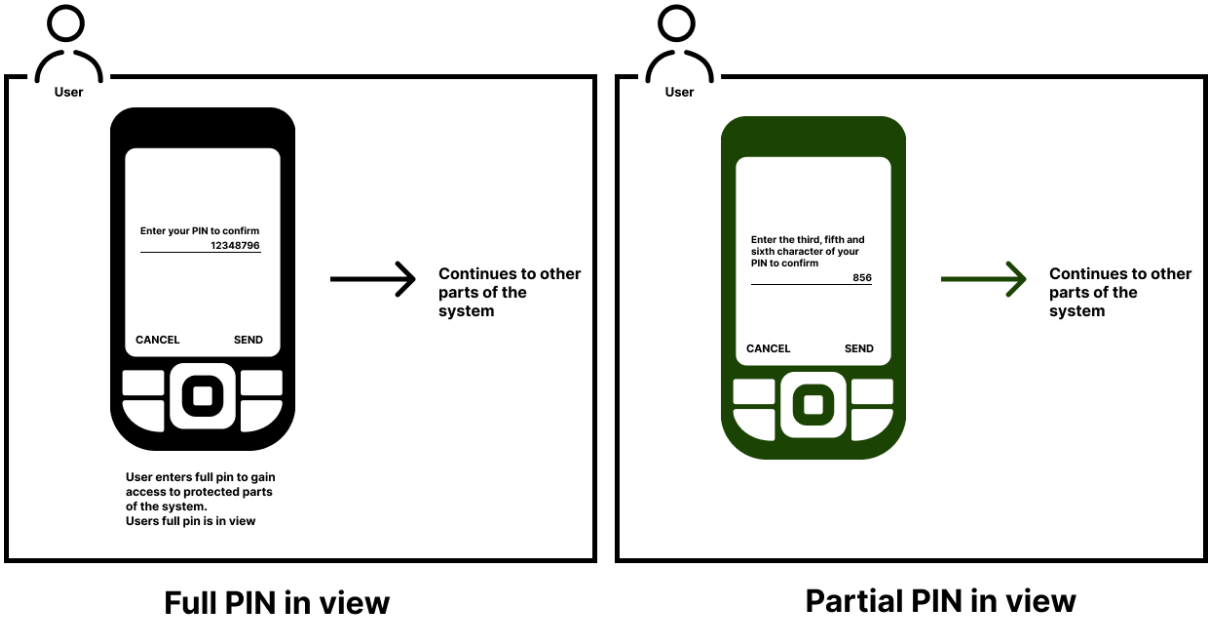

Figure 4.2 PIN entry contrast between existing implementation and solution implementation

Figure 4.2 depicts the pin entry in the existing implementation and proposed implementation interfaces. USSD system lacks input masking for PIN entry. This means sensitive information like PINs is displayed in plain text, making them vulnerable to shoulder-surfing attacks. Anyone observing the user in existing implementation during login or transaction could potentially steal their PIN. In contrast, in the proposed solution, the full PIN cannot be stolen even if the user is observed.

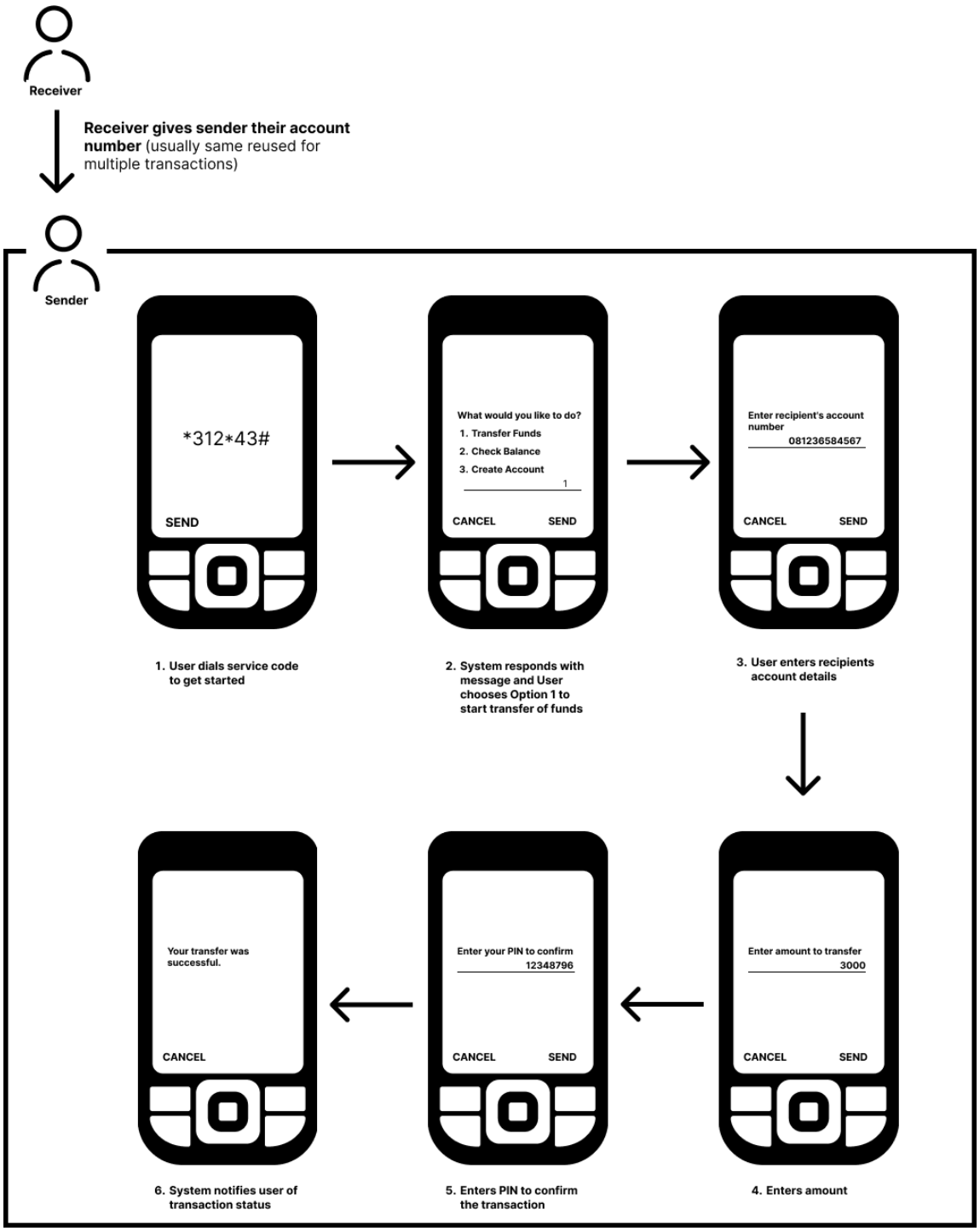

Figure 4.3 USSD Wireframes depicting the transfer flow for users in the existing implementation

Figure 4.3 illustrates a USSD session flow for a peer-to-peer (P2P) transaction using the existing implementation of the USSD digital wallet. In this process, the receiver shares their

account identifier, which is typically static and often their phone number. This static nature of the identifier makes it easy to recognise the receiver wherever those identifiers are used outside of the transaction, as mentioned in section 2.6.1

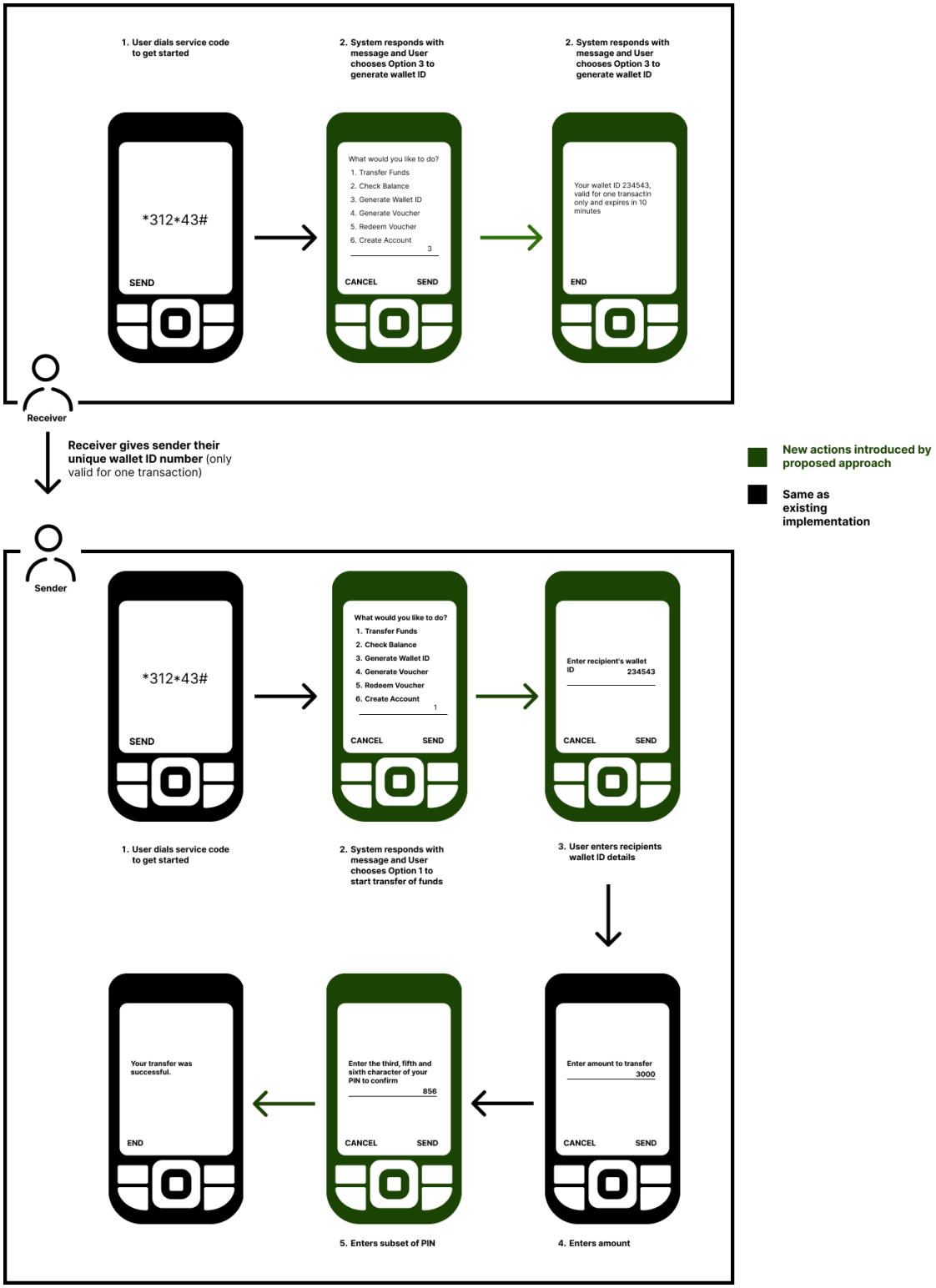

Figure 4.4 USSD Wireframes depicting the transfer flow for users in the proposed implementation

Figure 4.4 illustrates a USSD session flow for a peer-to-peer (P2P) transaction using the proposed solution for the USSD digital wallet. In this process, the receiver generates a unique wallet ID by dialling the USSD service code, choosing the right option and then sharing this ID with the sender. This prevents them from sharing any static information (account number or phone number) during the transaction. The sender also benefits from the partial PIN challenge during the transaction. These checks ensure improvements in security and user privacy concerns with existing implementations.

4.3.2 Use Cases

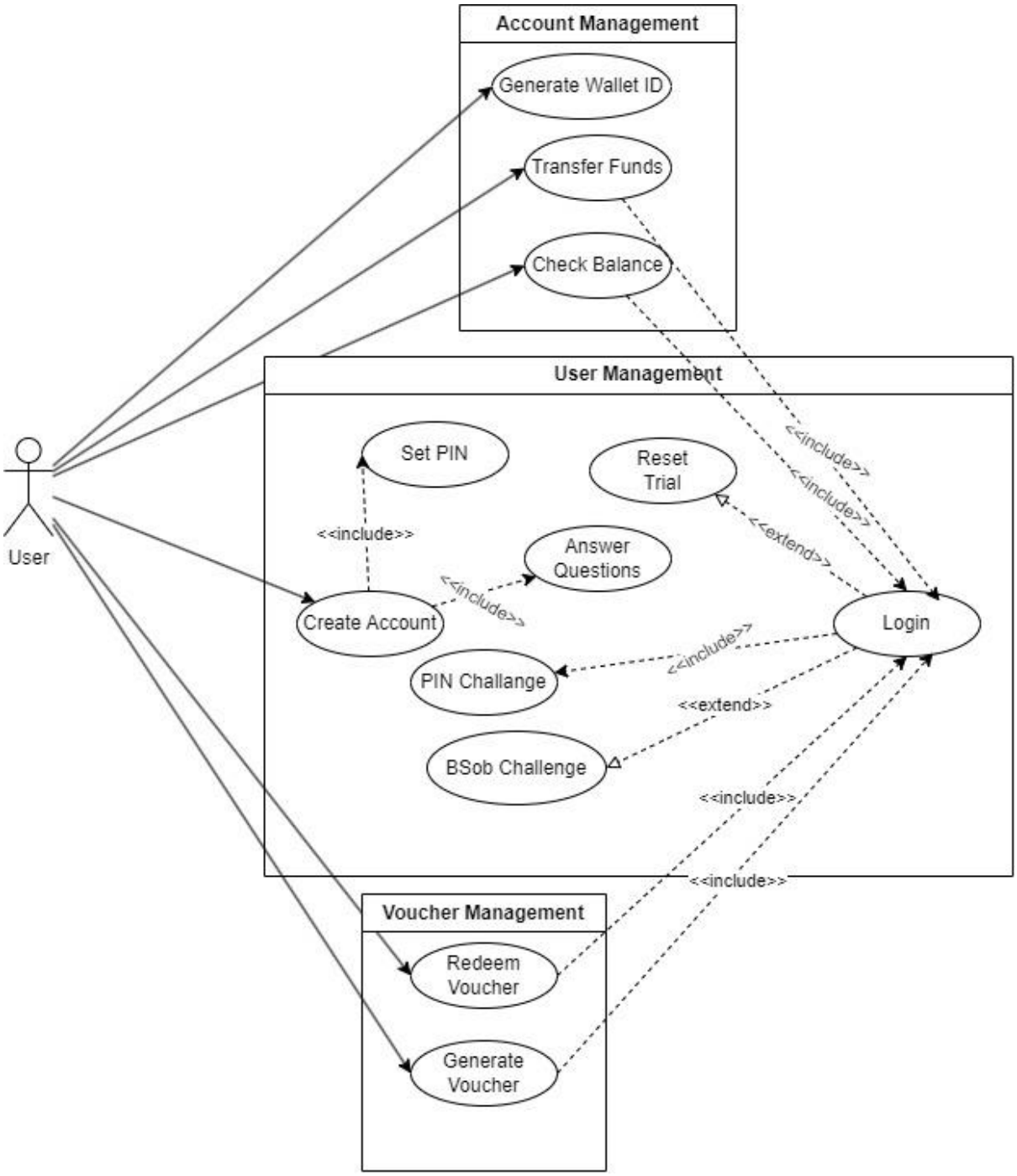

Figure 4.5 System Use Case

Figure 4.5 illustrates the basic functionalities of the system, with one primary actor (the user) and its relationship with the system's use cases.

4.3.3 ERD

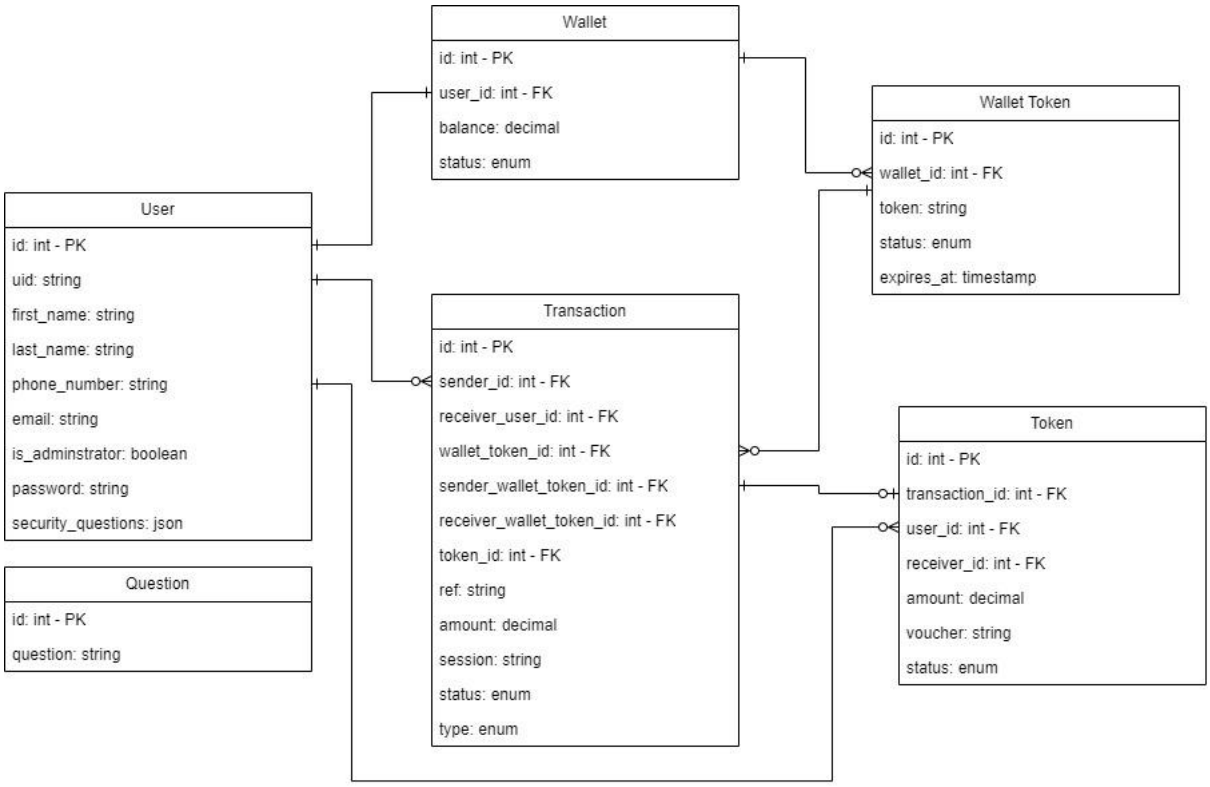

Figure 4.6 Entity Relationship Diagram

4.4 Prototype implementation and validation

4.4.1 Requirements

Table 4.1 Hardware Requirements

Hardware	Minimum Specifications	Recommended Specifications
Internet Connectivity	Required	Required
Disk Space	128 Gigabytes	1 Terabyte
Memory	2 Gigabytes	8 Gigabytes
Processor	1.0 Gigahertz (GHz), 64-bit	2.4 Gigahertz (GHz), 64-bit

Table 4.2 Software Requirements

Software	Minimum Specifications	Recommended Specifications
Operating System	Windows 7	Windows 10/CentOS/Ubuntu
Relational Database	MySQL 5.0	MySQL 8.3
In-Memory Database	Redis	Redis
Node Js environment	14.0	21.0

4.4.2 Auth Management

Handles the pin subset challenge and challenge questions

4.4.2.1 PIN subset challenge algorithm

The login algorithm leverages a random position challenge and hashed password storage. During registration, a user creates a PIN, and the system employs a hashing function (hashPassword) in Figure 4.7 to transform each character of the PIN into a distinct hash value. These hashed values are subsequently stored as an array within the database.

```
private async hashPassword(password: string): Promise<string> {
  const charHashes = []
  for (const char of password) {
    charHashes.push(await hash.make(char))
  }
  return JSON.stringify(charHashes)
}
```

Figure 4.7 HashPassword Function

During login, the user is prompted to enter three characters from random positions within their PIN. It's crucial to understand that the actual PIN characters are never stored directly. Instead, the system retrieves the pre-computed hash array associated with the user's account.

It then generates a set of random positions using the generateChallenge function shown in Figure 4.8 from within the PIN's length, excluding the first character for added security.

```
private generateChallenge(wordLength: number):number[] {
  const positions: number[] = []
  let attempts = 0
  while (positions.length < 3 && attempts < 10) {
    const position = Math.floor(Math.random() * (wordLength - 1)) + 1 // Exclude the first character for security
    if (!positions.includes(position)) {
      positions.push(position)
    }
    attempts++
  }
```

Figure 4.8 GenerateChallenge Function

For each requested position, the user's entered character is retrieved. The system then retrieves the corresponding hash value from the stored array based on the randomly generated position. A cryptographic verification function shown in Figure 4.9 then compares the hash of the entered character against the retrieved hash value. If the verification fails, the system increments a retry counter associated with the user's account. If the retry count is greater than or greater than 3, the user's account is temporarily blocked. The user is then prompted to

answer a pre-configured security question to regain access and reset the retry counter.

```
for (let i = 0; i < challengePositions.length; i++) {
  const verifiedChar = await hash.verify(
    parsedPassword[challengePositions[i]],
    request.pin[i]
  )
  if (!verifiedChar) {
    // INCREMENT RETRIES
    if (retries) {
      await redis.set(`retries-${request.phoneNumber}`, parseInt(retries) + 1)
    } else {
      await redis.set(`retries-${request.phoneNumber}`, 1)
    }
    this.response = 'END Incorrect characters, try again.'
    return this.response
  } else {
    await redis.del(`retries-${request.phoneNumber}`)
    await redis.del(`position-${user.id}`)
    console.log('successful login')
    this.response = 'SUCCESS'
    return this.response
  }
}
```

Figure 4.9 Verify PIN subset function

4.4.3 USSD Interfaces

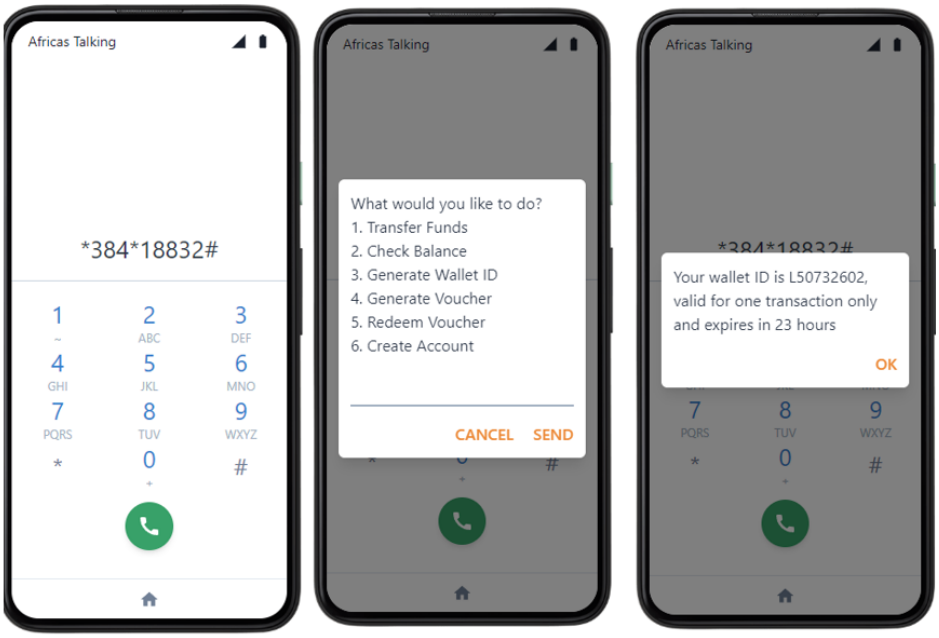

Figure 4.10 USSD Interface from Sandbox Simulation

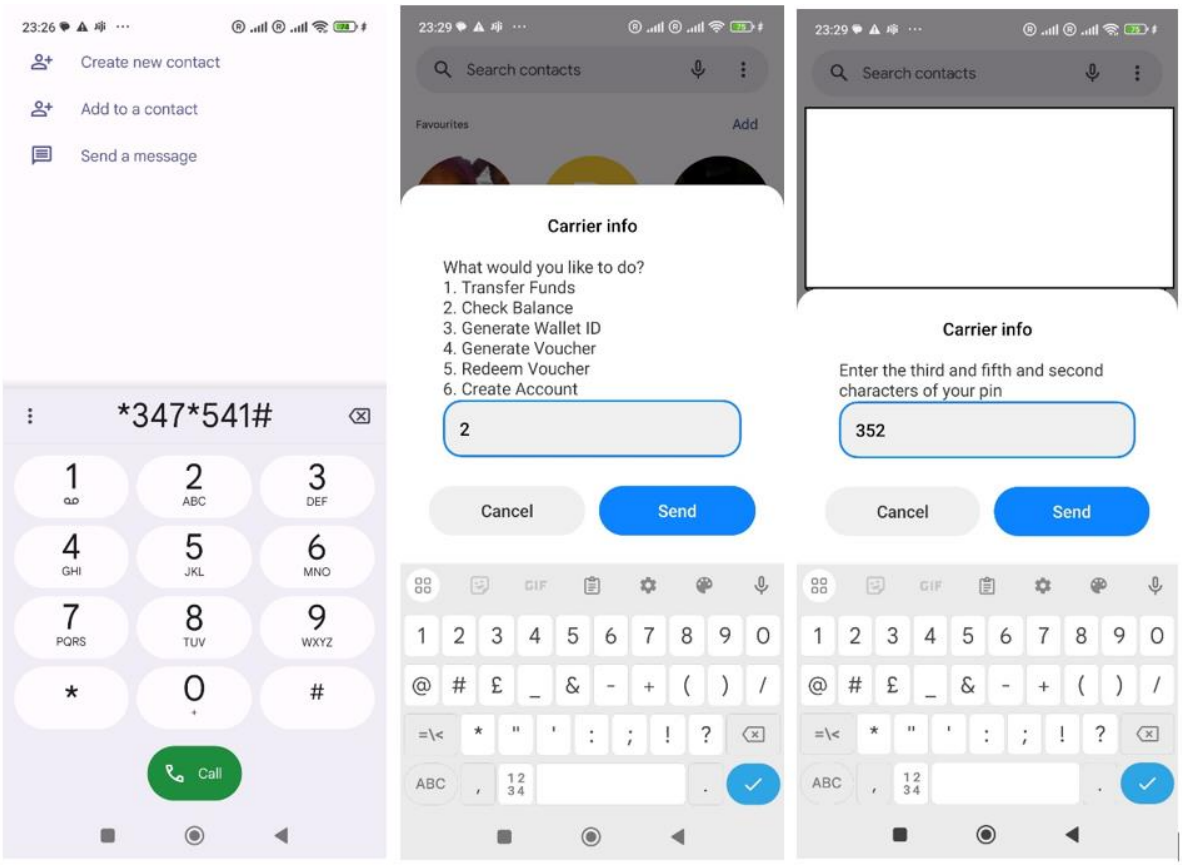

Figure 4.11 USSD Interface on a Real Device

4.4.4 API Testing

The test-driven approach in Agile methodology is a critical factor in ensuring customer satisfaction and good design habits (Ghanam et al., 2008). It involves the generation of test requirements from use case specifications, which is crucial for incremental coding (Tiwari & Gupta, 2015). The development process adopted an iterative approach, prioritising the completion of core functionalities to meet essential requirements before tackling more complex features. Through a series of refinements, it successfully passed the designed test cases. Table 4.3 provides a detailed breakdown of the test results.

Table 4.3 Test Case Report

No	Test	Action	Expected	Outcome

1	Automated load API testing.	Simulate multiple concurrent user logins.	Average response time between 200ms to 1000ms.	Pass
2	Account Block after Failed PIN Attempts.	Enter an incorrect Partial PIN three consecutive times.	Account gets locked	Pass
3	Prevent Self-Transfer	Attempt to send money to the same phone number linked to the account.	The system displays an error message indicating that self-transfer is not allowed	Pass
4	Security Questions for High-Risk Transactions.	Initiate a money transfer exceeding a predefined threshold	The user is prompted to answer pre-defined security questions	Pass
5	PIN Reset with Security Questions	After failing partial PIN attempts, answer security questions correctly	Account unlocks and allows PIN reset	Pass
6	USSD Session Timeout	The user remains inactive for an extended period (longer than idle time)	Session automatically terminates	Pass

7	Invalid Menu Input	Enter an invalid option within a USSD menu	The system displays an error message prompting the user to enter a valid option.	Pass
8	Insufficient Funds	Attempt to send money with an amount exceeding the available balance	The system displays an error message indicating adequate funds	Pass
9	Network Connectivity Test	Simulate a scenario with weak or no network connectivity	The system displays an error message indicating network connectivity issues	Pass
10	Invalid User Input	Enter invalid data during transactions (e.g., incorrect amount, non-numeric characters)	The user receives an error message with clear instructions	Pass

4.5 Critical Evaluation

4.5.1 Speed Evaluation with Real Devices

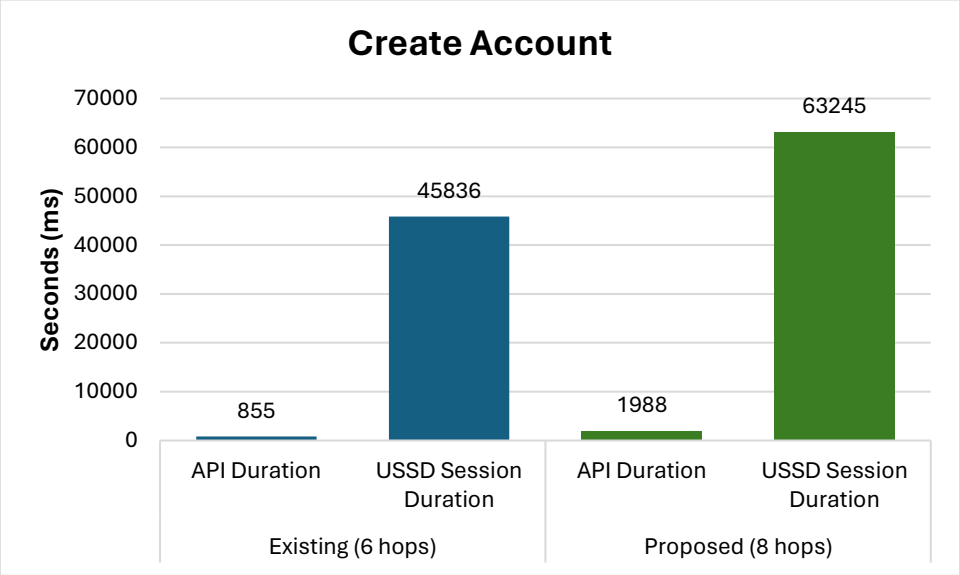

Figure 4.12 Duration of Existing and Proposed Implementation for Creating Accounts within the USSD Peer-to-Peer Transaction

The analysis of the USSD session logs reveals that creating an account takes less time with the existing implementation compared to the proposed one. This is because the proposed implementation introduces additional steps (2 extra hops) where users need to answer security questions. This results in an average increase of 132% in API response time and 38% in overall USSD session time compared to the existing implementation. The total USSD session is approximately 53% of the 120-second threshold.

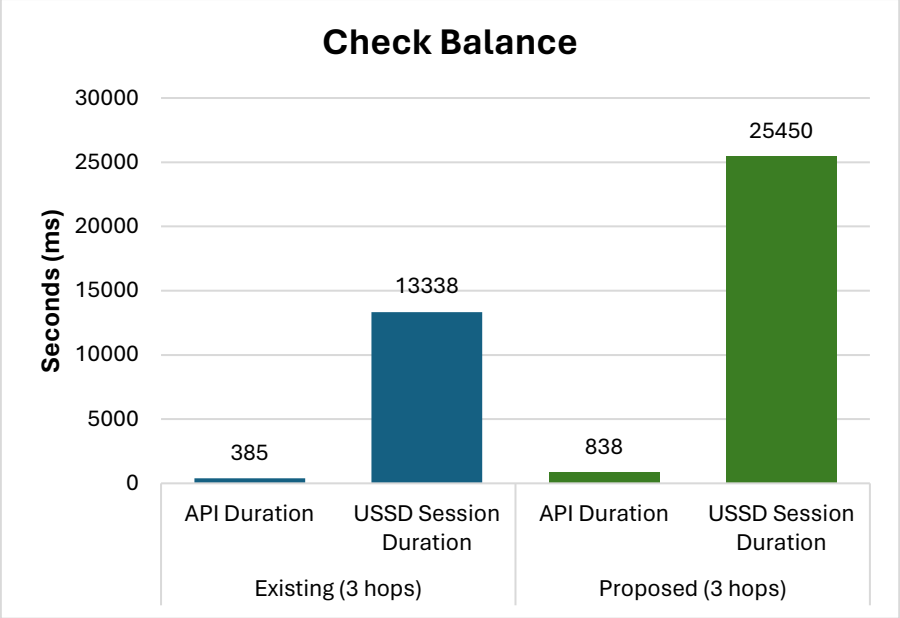

Figure 4.13 Duration of Existing and Proposed Implementation for Checking Balance within the USSD Peer-to-Peer Transaction

Figure 4.13 shows the proposed implementation, which shows an average of 116% increase in API response time and 88% increase in USSD session time compared to the existing implementation. The additional steps in the proposed implementation (2 extra hops) seem to be the reason for the significant increase in response and session time. These extra hops involve the security checks (Partial PIN challenge) that are not present in the existing implementation. The total USSD session is approximately 22% of the 120-second threshold.

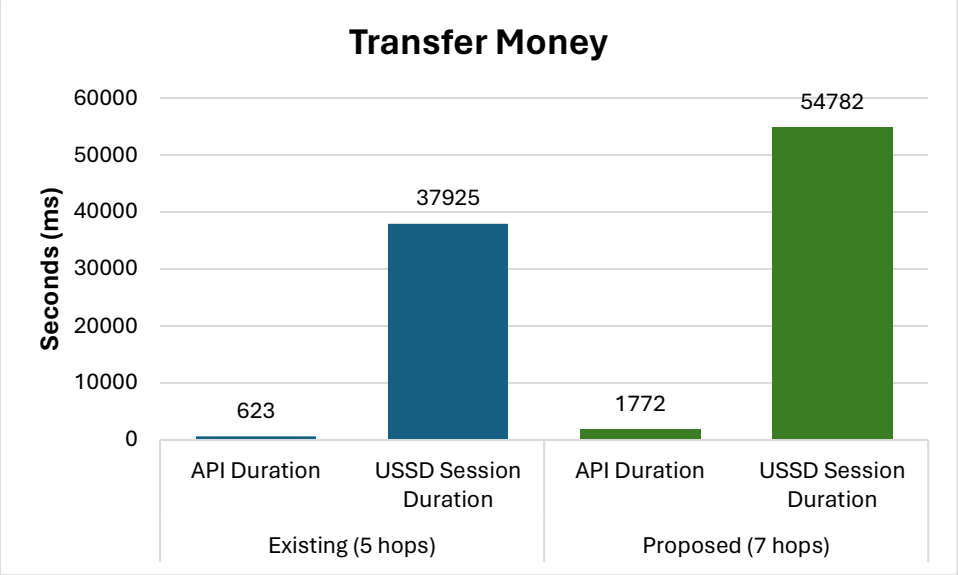

Figure 4.14 Duration of Existing and Proposed Implementation for Transferring Money within the USSD Peer-to-Peer Transaction

The graph in Figure 4.14 illustrates that the proposed money transfer implementation has a slower average response time (184% increase) and USSD session time (44% increase) compared to the existing implementation.

This difference can be attributed to the additional steps involved in the proposed approach. In the proposed implementation, the transferring of money is a combination of separate operations (Generate Wallet ID Operation in Figure 4.18 and the Transfer to Wallet Operation in Figure 4.19). Combining these durations reflects the overall time needed for the money transfer process in the proposed system.

While the proposed implementation takes longer, it remains within acceptable limits. The total USSD session time stays approximately 46% of the 120-second threshold (the permissible threshold to avoid session closure), and the user response time stays below 30 seconds (the customer response timeout limit).

In essence, the added security of the unique wallet ID comes at the cost of a bit more time, but the overall process remains efficient.

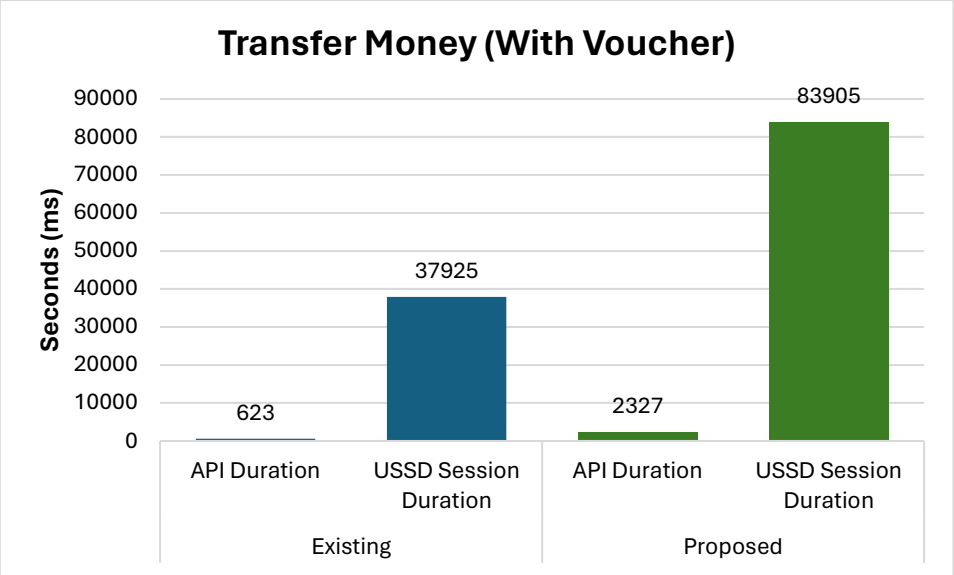

Figure 4.15 Duration of Existing and Proposed Implementation for transferring money (with vouchers) within the USSD Peer-to-Peer Transaction

The graph in Figure 4.15 shows a significant increase in both API response time (256% increase) and USSD session time (101% increase) for the proposed money transfer using vouchers compared to the existing implementation. However, it's important to note that the overall USSD session duration remains within acceptable limits, staying approximately 70% below the 120-second threshold.

This difference can be explained by the additional steps involved in the voucher system:

- **Unique Wallet ID generation:** The process starts with the receiver generating a unique wallet ID (Figure 4.18).
- **Voucher generation:** Once the ID is created, the sender initiates the money transfer using the ID, which then triggers voucher generation (Figure 4.20).
- **Voucher redemption:** Finally, the receiver redeems the voucher to complete the money transfer (Figure 4.21).

The total duration for the money transfer process in the proposed system is calculated by combining the times taken for these three individual steps. Although the proposed implementation takes considerably longer, it remains within acceptable limits. The USSD session stays under 120 seconds, the threshold to avoid session closure, and the user response time stays below 30 seconds, the customer response timeout limit.

The added security and control offered by using vouchers comes at the cost of increased processing time. However, the overall process remains functional within the acceptable timeframes for USSD sessions.

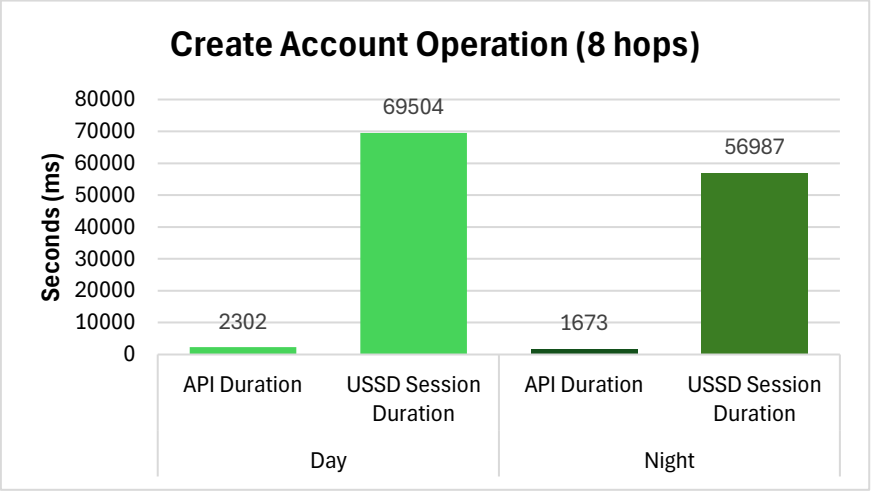

Figure 4.16 Day and Nighttime Durations for Create Account Operation within the Proposed USSD Peer-to-Peer Transaction

Daytime shows significantly better performance (faster API duration and USSD session duration) than nighttime. This difference could be due to higher network traffic during the night, impacting MNO response times.

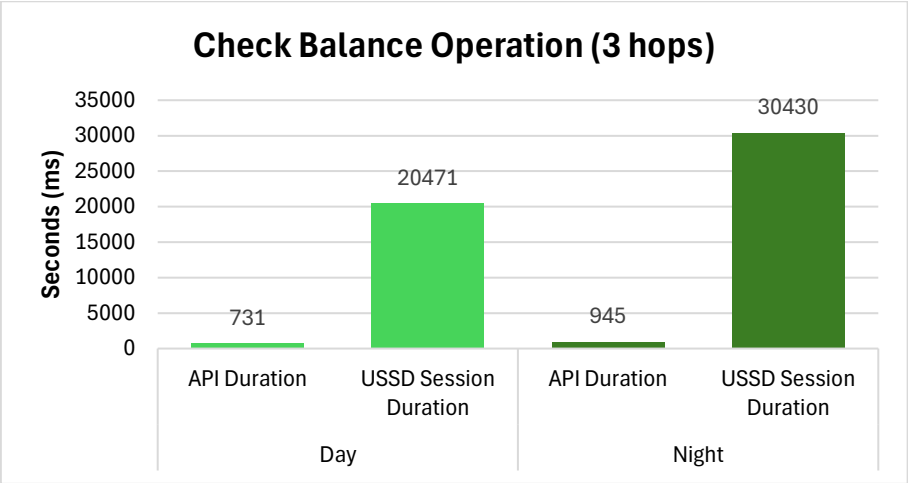

Figure 4.17 Day and Nighttime Durations for Check Balance Operation within the Proposed USSD Peer-to-Peer Transaction

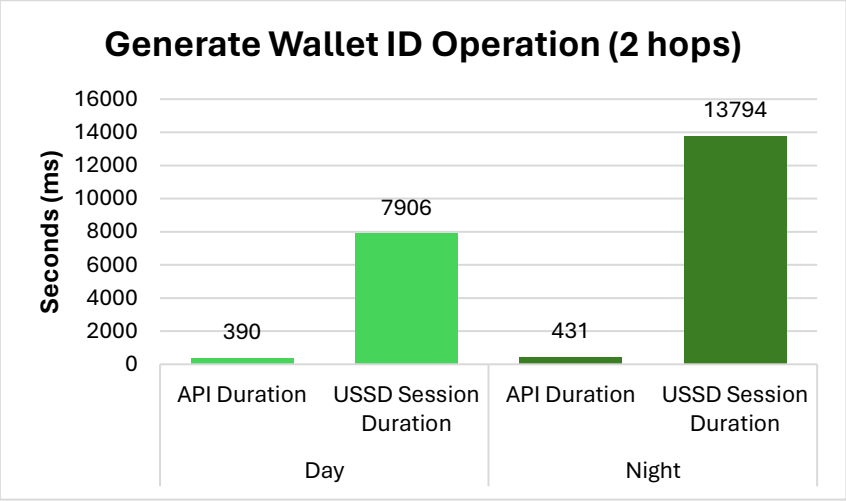

Figure 4.18 Day and Nighttime Durations for Generate Wallet ID Operation within the Proposed USSD Peer-to-Peer Transaction

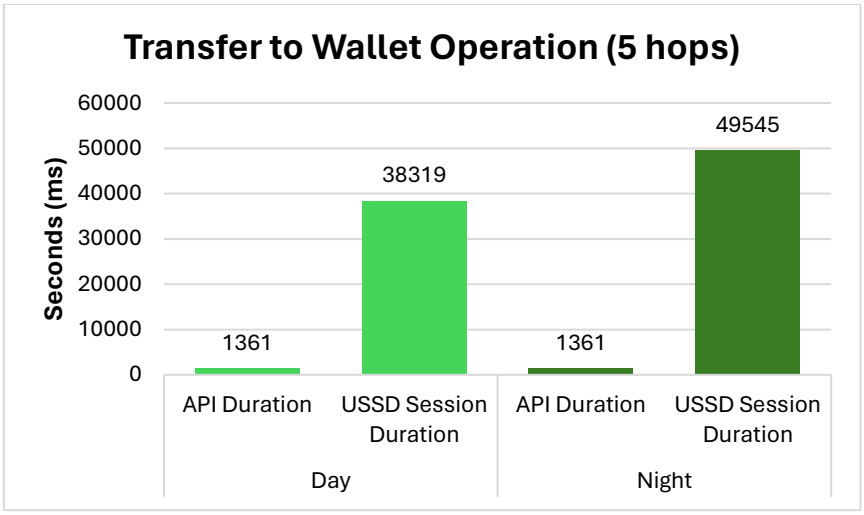

Figure 4.19 Day and Nighttime Durations for Transfer to Wallet Operation within the Proposed USSD Peer-to-Peer Transaction

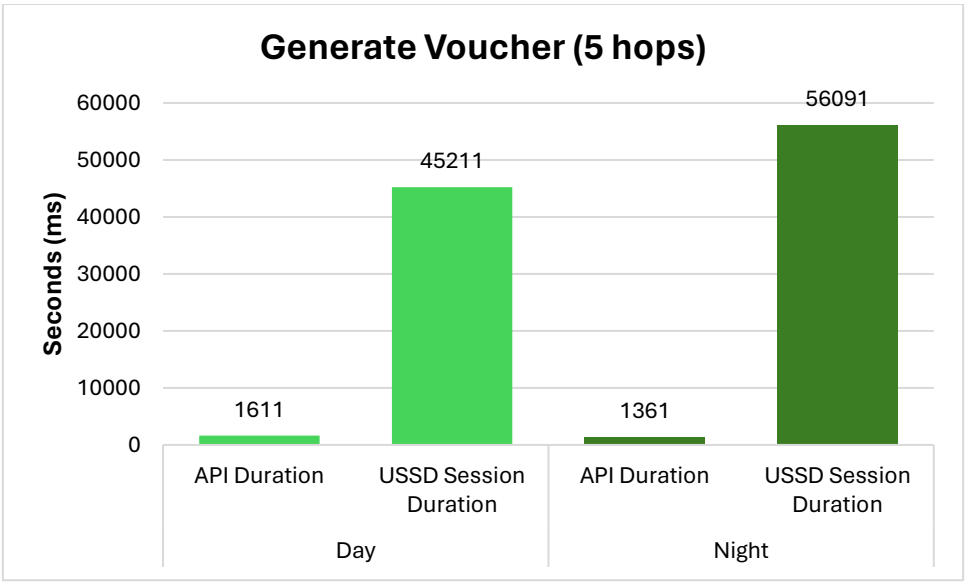

Figure 4.20 Day and Nighttime Durations for Generate Voucher Operation within the Proposed USSD Peer-to-Peer Transaction

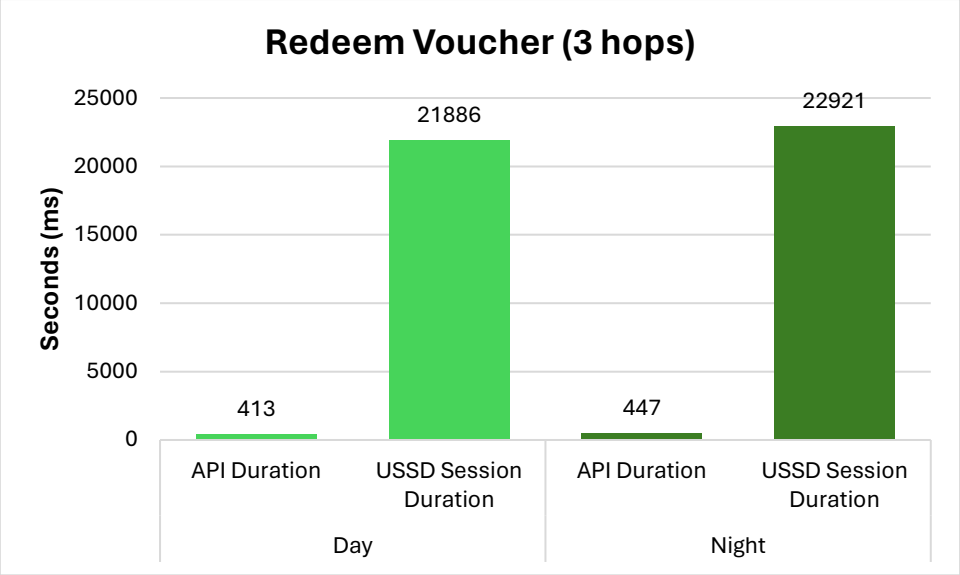

Figure 4.21 Day and Nighttime Durations for Redeem Voucher Operation within the Proposed USSD Peer-to-Peer Transaction

Across most operations, daytime sessions appear to be faster than nighttime sessions in terms of both API duration and USSD session duration. However, some inconsistencies suggest potential network variations. While daytime generally shows better performance, the observed inconsistencies between day and night for several operations (increased USSD session duration at night) suggest that MNO network performance might be a contributing factor. A higher network traffic could cause these inconsistencies at night. Increased user activity at night could lead to network congestion, impacting response times for both USSD services and user interactions with the USSD menus.

4.5.2 Simulation vs Real Device

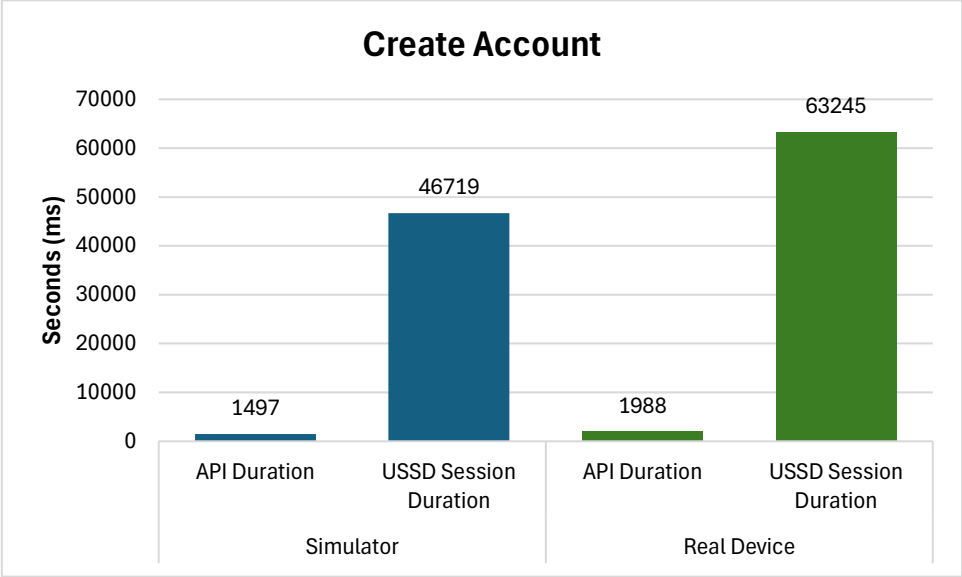

Figure 4.22 Session Duration Comparison between Simulated and Real Device Tests for Creating Account.

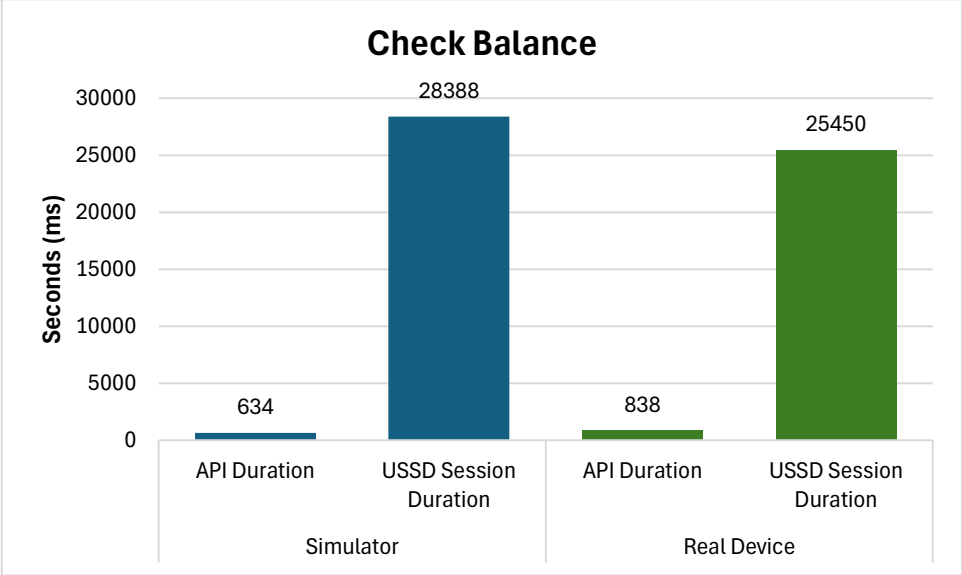

Figure 4.23 Session Duration Comparison between Simulated and Real Device Tests for Checking Balance.

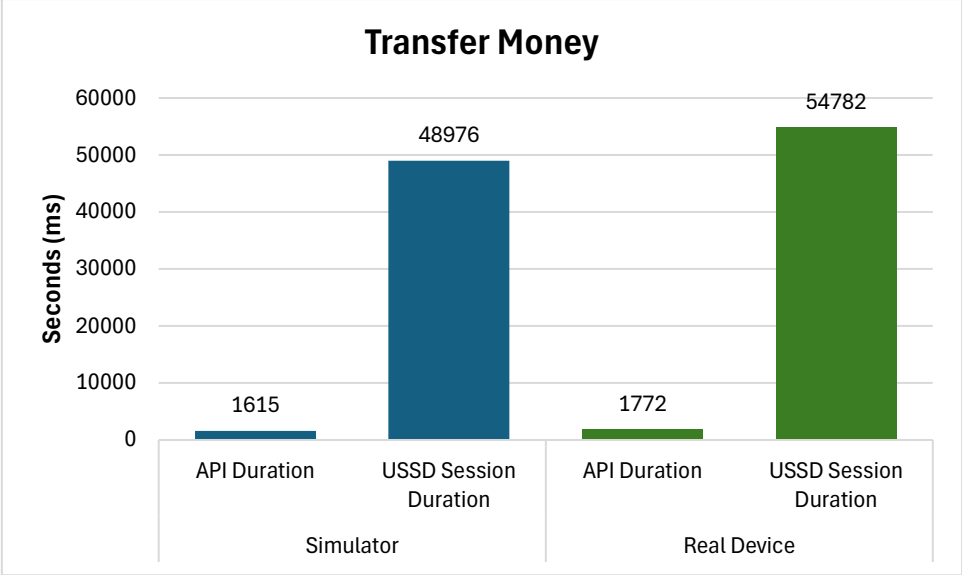

Figure 4.24 Session Duration Comparison between Simulated and Real Device Tests for Transferring Money.

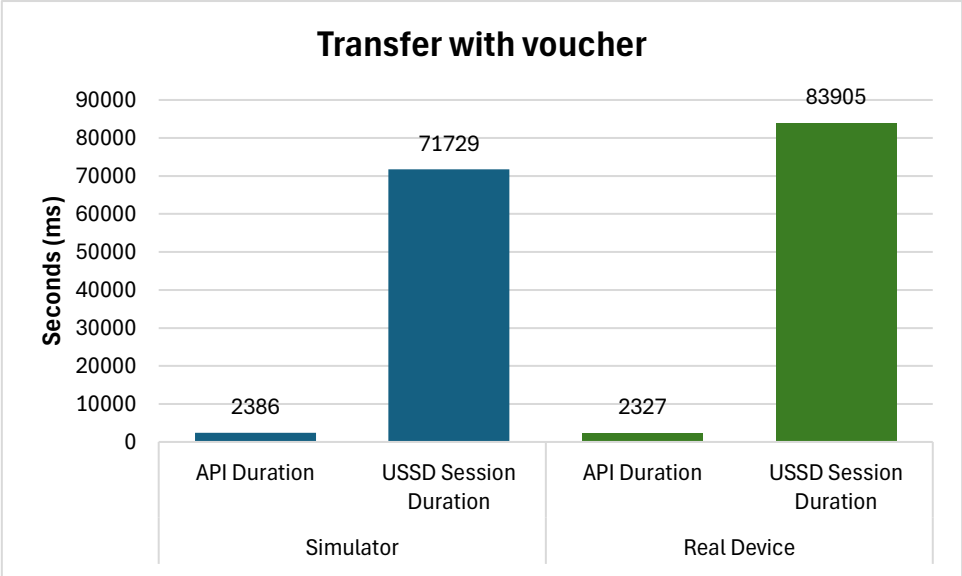

Figure 4.25 Session Duration Comparison between Simulated and Real Device Tests for Transferring Money with Voucher.

In all four operations (Create Account, Check Balance, Transfer Money, Transfer with Voucher), real devices consistently show longer session durations compared to simulated devices. This could be a result of the following reasons:

Network Variations: Real-world network conditions introduce latency into data transmission between the user device, MNO network, and USSD gateway.

User Input Delays: Real users might take more time to read USSD menus, understand information, and type responses compared to simulated tests, as the simulated tests were carried out by testers who developed the platform and have spent a considerable amount of time already testing the application.

4.5.3 Security Evaluation

The testing demonstrated that the Partial PIN method effectively enhances the security of the USSD digital wallet compared to existing systems requiring full PIN entry. All simulated hacking attempts, where users tried to access another's account with only three provided PIN characters, resulted in account lockout after three trials.

This contrasts with existing systems requiring full PIN entry, where a single successful guess grants complete access. The Partial PIN method adds an extra layer of security, making it significantly harder for unauthorised individuals to gain access to user accounts.

4.5.4 User Experience Evaluation

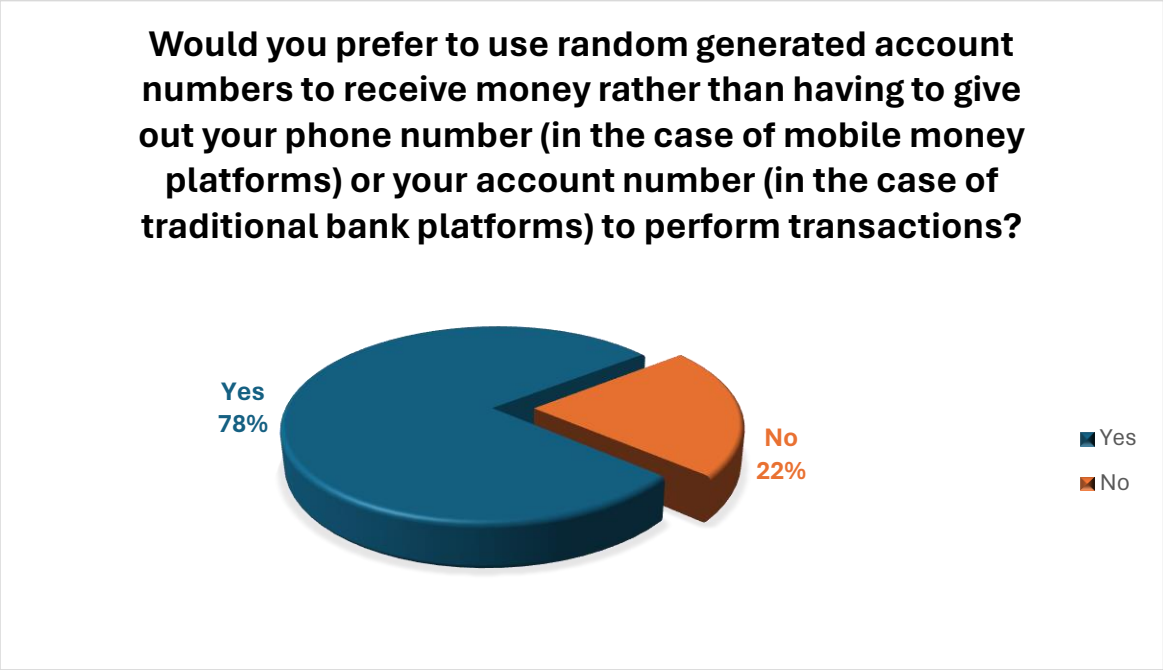

Figure 4.26 Users Preference for Random Generate Wallet IDs.

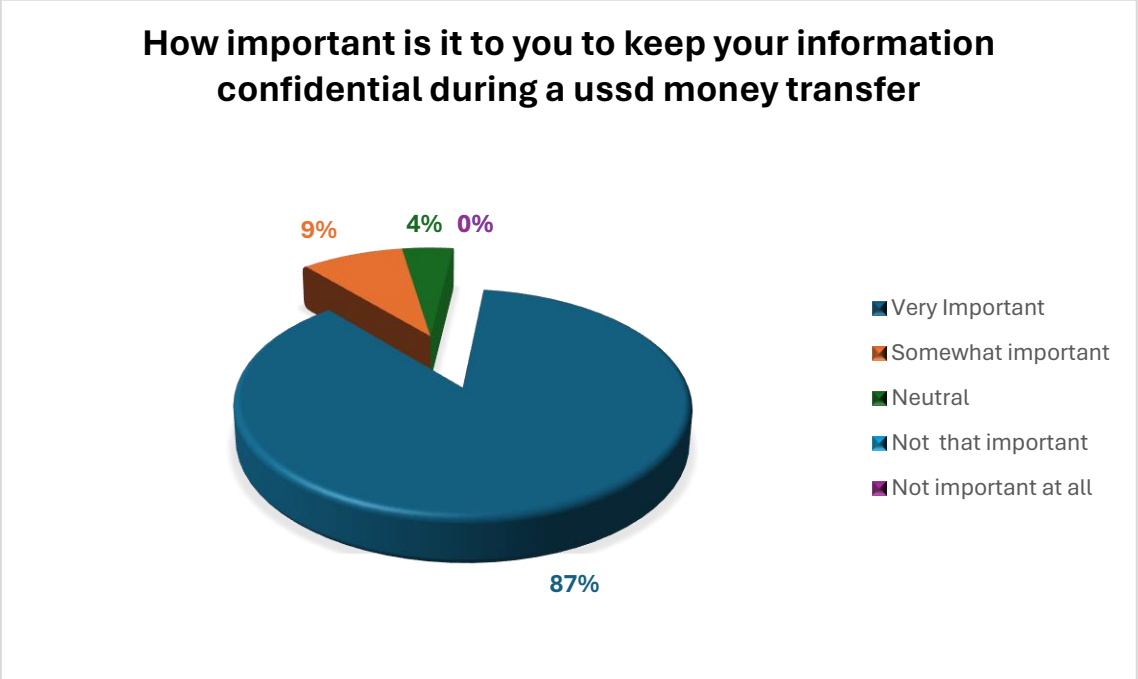

Figure 4.27 Users' Preference for Privacy in USSD Peer-to-Peer Transactions

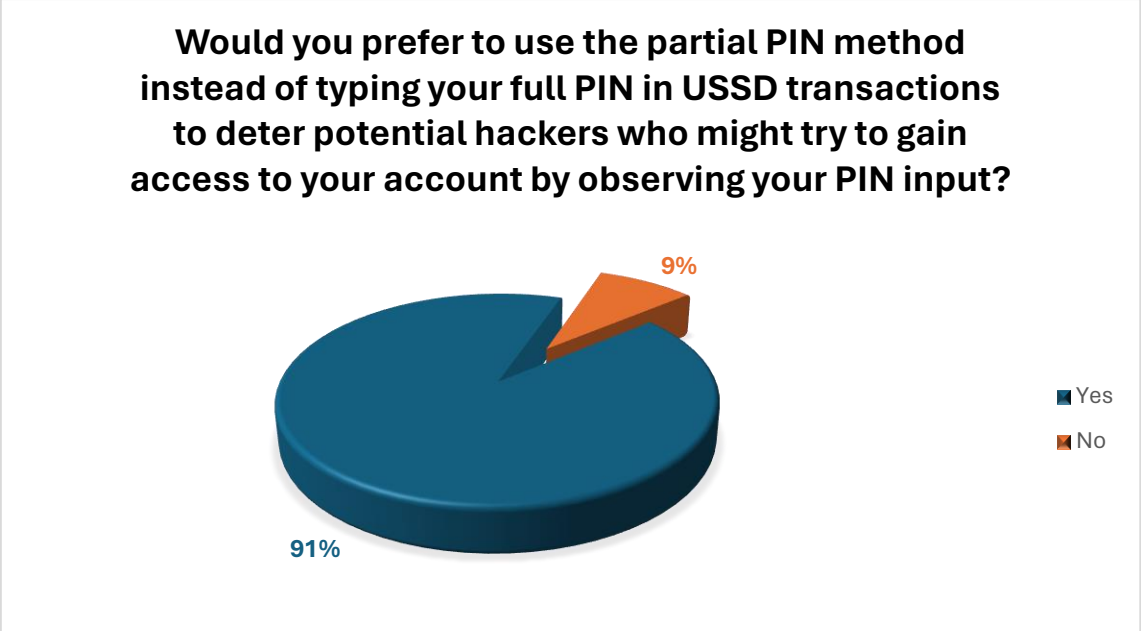

Figure 4.28 Users' Preference for the Partial PIN Method as Compared to the Full PIN Method

A significant majority (87%) consider keeping their information confidential during USSD money transfers to be very important. This highlights the user's strong emphasis on data privacy and security.

78% of users prefer randomly generated account numbers for receiving money over sharing phone numbers or traditional account numbers. This suggests a desire for increased security and control over personal information. Reasons cited include:

- **Reduced risk of exposing phone numbers:** This aligns with the desire for privacy and potentially avoids unwanted calls or messages.
- **Reduced risk of errors:** Avoiding phone number sharing minimises the possibility of accidentally entering incorrect digits.

A large majority (91%) prefer the partial PIN method for entering their PIN during USSD transactions. This indicates a strong preference for a security mechanism that reduces the risk of someone observing and stealing their full PIN.

The user responses indicate a strong focus on security and privacy when it comes to USSD money transfers. The use of unique wallet IDs and partial PIN methods will likely improve overall user experience and trust in the system. However, addressing potential concerns through clear communication can further enhance user adoption.

5 Conclusion and Future Work

This study aimed to address the limitations of existing USSD-based payment systems that are adaptable to basic feature phones. The research investigated current USSD usage for payment transactions, assessed security vulnerabilities, and designed a secure offline P2P payment system utilising strong authentication while preserving user anonymity.

The analysis revealed several key issues with existing USSD-based payment models. Sharing phone numbers as identifiers exposes users to privacy risks due to social engineering attacks and the limitations of GDPR compliance. Additionally, the reliance on PIN-based authentication is susceptible to brute-force attacks and shoulder surfing, especially with the lack of masked input in USSD's text-based format. Furthermore, existing research tends to focus on replicating mobile payment models within USSD's limitations, neglecting the exploration of alternative P2P-specific approaches.

5.1 Recommendations

The analysis revealed that the proposed USSD system offers a secure and efficient platform for financial transactions on basic feature phones. The implementation of the partial PIN method significantly enhances security compared to traditional full PIN entry, deterring unauthorised access attempts. Additionally, the system adheres to acceptable USSD session duration limits, ensuring a smooth user experience. However, there's potential to optimise the system further based on user preferences and address network variations.

5.2 Further Works

- **Improved Accessibility for Basic Feature Phones:**

- Implement a system allowing users of basic feature phones without QWERTY keypads to answer security questions using numerical responses instead of letters. This can significantly improve accessibility for a broader user base.

- **Customizable Security Questions:**
    - Explore the feasibility of allowing users to choose their security questions during registration. This could potentially reduce the time spent registering for USSD sessions if users can select questions with readily recalled answers. The effectiveness of this feature should be evaluated through user testing to confirm if it reduces registration time without compromising security.
- **Enhanced PIN Security:**
    - Investigate implementing a mechanism to limit PIN retry attempts after a certain threshold. This could involve requiring admin intervention to unlock accounts after multiple failed attempts. However, this approach necessitates a method for users to provide additional information beyond their PIN to verify their identity during the unlocking process. This additional information could be collected during initial account creation and securely stored. This balance between enhanced security and user experience needs careful consideration.
- **Lost/Stolen Phone Reporting:**
    - Develop a mechanism within the USSD system for users to report lost or stolen phones associated with their accounts. This should ideally involve a secure way to deactivate the account and potentially link it to a new device.
- **Network Performance Analysis:**

- Conduct further investigation to understand the root cause of inconsistencies observed in performance between daytime and nighttime USSD sessions. This could involve analysing additional network performance metrics beyond just response times, such as packet loss rates. Additionally, gathering user feedback about potential network-related issues during nighttime sessions could provide valuable insights. By comprehensively understanding the impact of network variations, strategies can be developed to optimise performance across different periods.

Overall, by implementing these recommendations and conducting further research, the USSD digital wallet system can be refined to provide a more secure, accessible, and user-friendly platform for financial transactions on basic feature phones.

6 References

Adonis JS Lucid (2024). *Database seeders*. [Online]. 2024. Available from: https://lucid.adonisjs.com. [Accessed: 28 April 2024].

Africa's Talking (2024). *Africa's Talking – Communication APIs for Africa*. [Online]. 2024. Available from: https://africastalking.com/. [Accessed: 28 April 2024].

Bairagi, V. & Munot, M.V. (2019). Research Methodology. *Storytelling with Data in Healthcare*. [Online]. Available from: https://api.semanticscholar.org/CorpusID:6410019.

Baltes, S. & Ralph, P. (2021). *Sampling in Software Engineering Research: A Critical Review and Guidelines*. [Online]. Available from: http://arxiv.org/abs/2002.07764. [Accessed: 28 April 2024].

Binbeshr, F., Mat Kiah, M.L., Por, L.Y. & Zaidan, A.A. (2021). A systematic review of PIN-entry methods resistant to shoulder-surfing attacks. *Computers & Security*. 101. p.p. 102116.

Binbeshr, F., Por, L.Y. & Kiah, M.L.M. (2023). *Challenge-Response Pin Authentication System to Withstand Shoulder Surfing and Recording Attacks*. [Online]. Available from: https://papers.ssrn.com/abstract=4625444. [Accessed: 18 March 2024].

Binitie, A.P., Innocent, O.S., Egbokhare, F. & Egwali, A.O. (2021). Implementing Existing Authentication Models In USSD Channel. In: *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*. [Online]. 9 December 2021, Cape Town, South Africa: IEEE, pp. 1–5. Available from: https://ieeexplore.ieee.org/document/9698659/. [Accessed: 16 February 2024].

Bo A. V. Äström & Björn A. Svennesson (1998). *Unstructured Supplementary Service Data From a Home Location Register to an External Node*. [Online]. p.p. 13. Available from: https://ppubs.uspto.gov/dirsearch-public/print/downloadPdf/5752188. [Accessed: 14 March 2024].

Bullée, J.-W., Montoya, L., Junger, M. & Hartel, P.H. (2016). *Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention*. In: 2016, IOS Press, pp. 107–114.

Clarke, E. & Visser, J.W. de (2018). Pragmatic research methodology in education: possibilities and pitfalls. *International Journal of Research & Method in Education*. 42. p.pp. 455–469.

Cormack, A. (2020). *An Introduction to the GDPR*. In: [Online]. 31 March 2020. Available from: https://www.semanticscholar.org/paper/An-Introduction-to-the-GDPR-Cormack/1787ca85f1d2735875cef47d64487c10e213d1a1. [Accessed: 28 April 2024].

Cormack, A. (2021). An Introduction to the GDPR (v2). *IDPro Body of Knowledge*. [Online]. 1 (5). Available from: https://bok.idpro.org/article/id/11/. [Accessed: 28 April 2024].

Dayang, P. & Hamza, A. (2021). Using USSD-based Mobile Payment in Context of Low Internet Connection. *International Journal of Wireless Communications and Mobile Computing*. 9 (1). p.pp. 1–6.

Emerson, R.S.W. (2021). Convenience Sampling Revisited: Embracing Its Limitations Through Thoughtful Study Design. *Journal of Visual Impairment & Blindness*. 115. p.pp. 76–77.

European Telecommunications Standards Institute (1997). *Digital cellular telecommunications system; Unstructured Supplementary Service Data (USSD) - Stage 1 (GSM 02.90)*. [Online]. Available from: https://www.etsi.org/deliver/etsi_gts/02/0290/05.01.00_60/gsmts_0290v050100p.pdf. [Accessed: 11 March 2024].

Ghanam, Y., Park, S. & Maurer, F. (2008). A Test-Driven Approach to Establishing & Managing Agile Product Lines. In: *Software Product Lines Conference*. [Online]. 2008. Available from: https://api.semanticscholar.org/CorpusID:18924205.

Grady, J.O. (2007). *Requirements Analysis Overview*. In: [Online]. 2007. Available from: https://api.semanticscholar.org/CorpusID:60164229.

Hussaini, A.Z., Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology, Minna, Niger, Nigeria, Suleiman, A.D., Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology, Minna, Niger, Nigeria, Stella, O.E., Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology, Minna, Niger, Nigeria, Faiza, B.J., Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology, Minna, Niger, Nigeria, Idris, M.K., & Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Minna, Niger, Nigeria (2020). A USSD BASED CASHLESS REVENUE COLLECTION SYSTEM: TARGETING THE INFORMAL SECTOR. *i-manager's Journal on Information Technology*. 9 (1). p.p. 22.

Islam, M. (2020). Data Analysis: Types, Process, Methods, Techniques and Tools. *International Journal on Data Science and Technology*. [Online]. Available from: https://api.semanticscholar.org/CorpusID:212873754.

Jakobsson, M. & Liu, D. (2013). *Your Password is Your New PIN*. In: [Online]. 2013. Available from: https://api.semanticscholar.org/CorpusID:59844468.

Kumar, D.V. & Sowmyavani, M.M. (2012). *Agile Software Development : A Case Study of Web Application*. In: [Online]. 2012. Available from: https://api.semanticscholar.org/CorpusID:35663006.

Kumar, V., Anand, A. & Song, H. (2017). Future of Retailer Profitability: An Organizing Framework. *Journal of Retailing*. 93 (1). p.pp. 96–119.

Lakshmi, K.K., Gupta, H. & Ranjan, J. (2017). USSD — Architecture analysis, security threats, issues and enhancements. In: *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*. [Online]. December 2017, pp. 798–802. Available from: https://ieeexplore.ieee.org/document/8286115. [Accessed: 12 February 2024].

Lamoyero, Z. & Fajana, O. (2023). Exposed: Critical Vulnerabilities in USSD Banking Authentication Protocols. In: *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. [Online]. July 2023, pp. 275–280. Available from: https://ieeexplore.ieee.org/abstract/document/10224933?casa_token=6jGiSw0pciwAAAAA:r0w2k21BMg__3ISVmDDlPNwAo4r0TyWWpX-O-_NybVRCmOovg-xgUic05CrK9GZZsKUAEflg. [Accessed: 27 April 2024].

Mallik, A., Tran, C. & Twagirumukiza, A. (2020a). USSD Digital Wallet. In: *2020 Intermountain Engineering, Technology and Computing (IETC)*. October 2020, pp. 1–5.

Mallik, A., Tran, C. & Twagirumukiza, A. (2020b). USSD Digital Wallet. In: *2020 Intermountain Engineering, Technology and Computing (IETC)*. [Online]. 2 October 2020, Orem, UT, USA: IEEE, pp. 1–5. Available from: https://ieeexplore.ieee.org/document/9249106/. [Accessed: 12 February 2024].

McDonald, A., Sugatan, C., Guberek, T. & Schaub, F. (2021). The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. [Online]. Available from: https://api.semanticscholar.org/CorpusID:233987827.

Nandakumar, K. & Jain, A.K. (2009). Soft Biometrics. In: S. Z. Li & A. Jain (eds.). *Encyclopedia of Biometrics*. [Online]. Boston, MA: Springer US, pp. 1235–1239. Available from: https://doi.org/10.1007/978-0-387-73003-5_225. [Accessed: 18 March 2024].

Neza, F. & Joseph, A.J. and M. (2022). *E-MONEY SECURITY DILEMMA: ADVANCED CYBERSECURITY MECHANISMS AND LEGACY MOBILE PAYMENTS IN SUB-SAHARAN AFRICA*. In: [Online]. 2022, pp. 103–114. Available from: https://www.iadisportal.org/digital-library/e-money-security-dilemma-advanced-cybersecurity-mechanisms-and-legacy-mobile-payments-in-sub-saharan-africa. [Accessed: 11 April 2024].

Njuguna Michael (2020). *Dynamic Knowledge Based Authentication Model for Enhancing Security of USSD Banking Transactions*.

Nyamtiga, B.W., Sam, A. & Laizer, L.S. (2013). Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania. *International Journal of Technology Enhancements and Emerging Engineering Research*. [Online]. Available from: https://www.semanticscholar.org/paper/Security-Perspectives-For-USSD-Versus-SMS-In-Mobile-Nyamtiga-Sam/9408b82cc059e5f10b6aca19b66cf224aee4adee. [Accessed: 16 February 2024].

Olamilekan, O., Adedoyin, A. & Abdukareem, S.A. (2022). Design and Simulation of Unstructured Supplementary Service Data (USSD) to Fund Bank Accounts using Mobile Recharge Credit Vouchers. *Adeleke University Journal of Engineering and Technology*. 5 (2). p.pp. 29–38.

Otor, S.U., Akumba, B.O., Idikwu, J.S. & Achika, I.P. (2020). An Improved Security Model for Nigerian Unstructured Supplementary Services Data Mobile Banking Platform. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. p.pp. 974–987.

Owusu, B., Atta, N., Ben, J. & Vormawor, C. (2018). Improving Electronic Banking in Ghana using USSD. *International Journal of Computer Applications*. 180 (17). p.pp. 8–13.

Patience, A., Christiana, N. & Oguguo, P. (2022). *Security against Shoulder Surfing Attack Adaptable to Feature Phones using USSD Technology*. 7 (12).

Perrier, T., DeRenzi, B. & Anderson, R. (2015). USSD: The Third Universal App. In: *Proceedings of the 2015 Annual Symposium on Computing for Development*. DEV '15. [Online]. 1 December 2015, New York, NY, USA: Association for Computing Machinery, pp. 13–21. Available from: https://dl.acm.org/doi/10.1145/2830629.2830645. [Accessed: 20 February 2024].

Perrier, T., Yu, S. & Anderson, R. (2016). UW-Pesa: A Mobile Money User Experience Experimentation Platform. In: *Proceedings of the 7th Annual Symposium on Computing for Development*. ACM DEV '16. [Online]. 18 November 2016, New York, NY, USA:

Association for Computing Machinery, pp. 1–4. Available from: https://dl.acm.org/doi/10.1145/3001913.3006650. [Accessed: 15 April 2024].

O. Radley-Gardner, H. Beale, & R. Zimmermann (eds.) (2016). *Fundamental Texts On European Private Law*. [Online]. Hart Publishing. Available from: http://www.bloomsburycollections.com/book/fundamental-texts-on-european-private-law-1. [Accessed: 16 April 2024].

Ramli, F.A.A. & Hamzah, M.I. (2021). Mobile payment and e-wallet adoption in emerging economies: A systematic literature review. *Journal of Emerging Economies and Islamic Research*. 9 (2). p.pp. 1–39.

Sheil, A. & Malone, D. (2022). Guessing PINs, One Partial PIN at a Time. *Entropy*. 24 (9). p.p. 1224.

Somtochukwu Anunobi (2024). *USSD Digital wallet with PIN authentication*. [Online]. Available from: https://github.com/somteacodes/usepay1.0. [Accessed: 12 May 2024].

Song, X., Wang, X., Nie, L., He, X., Chen, Z. & Liu, W. (2018). A Personal Privacy Preserving Framework: I Let You Know Who Can See What. In: *The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval*. SIGIR '18. [Online]. 27 June 2018, New York, NY, USA: Association for Computing Machinery, pp. 295–304. Available from: https://dl.acm.org/doi/10.1145/3209978.3209995. [Accessed: 15 April 2024].

Sukmawati, S., Sudarmin (2023). DEVELOPMENT OF QUALITY INSTRUMENTS AND DATA COLLECTION TECHNIQUES. *Jurnal Pendidikan dan Pengajaran Guru Sekolah Dasar (JPPGuseda)*. [Online]. Available from: https://api.semanticscholar.org/CorpusID:258425091.

Telegram (2024). *Telegram – a new era of messaging*. [Online]. 2024. Telegram. Available from: https://telegram.org/?setln=en. [Accessed: 10 May 2024].

Tiwari, S. & Gupta, A. (2015). An Approach of Generating Test Requirements for Agile Software Development. *Proceedings of the 8th India Software Engineering Conference*. [Online]. Available from: https://api.semanticscholar.org/CorpusID:2791361.

Vinay Kumar B (2022). Authorization and Authentication in Mobile Devices. *International Journal for Research in Applied Science and Engineering Technology*. 10 (4). p.pp. 1733–1738.

Vugdelija, N., Nedeljković, N., Kojić, N., Lukić, L. & Vesić, M. (2021). *Review of brute-force attack and protection techniques*. In: 2021, pp. 220–230.

Wavinya, C. (2024). *How long is the duration of a USSD session for Nigerian Telcos ? | Africa's Talking Help Center*. [Online]. 2024. Available from: https://help.africastalking.com/en/articles/2298298-how-long-is-the-duration-of-a-ussd-session-for-nigerian-telcos. [Accessed: 10 May 2024].

World Bank Group (2021). *The Global Findex 2021: Interactive Executive Summary Visualization*. [Online]. 2021. World Bank. Available from: https://www.worldbank.org/en/publication/globalfindex/interactive-executive-summary-visualization. [Accessed: 9 April 2024].

Wycliffe Ochieng' Agwanyanjaba (2020). *Enhanced Mobile Banking Security: Implementing Transaction Authorization Mechanism Via Ussd Push.*

Appendix A: Links

UsePay test Telegram Bot https://github.com/somteacodes/usepaybot

Proposed Implementation https://github.com/somteacodes/usepay2.0

Existing implementation https://github.com/somteacodes/usepay1.0

Appendix B: Abbreviations

MNO: Mobile Network Operator

USSD: Unstructured Supplementary Service Data

BOSB: Bag of Soft Biometrics

OTP: One-Time Password

GDPR: General Data Protection Regulation

KBA: Knowledge-Based Authentication

P2P: Peer-to-Peer

MFA: Multi-Factor Authentication

Appendix C: Research Budget

Estimated research costs

Item	Type	Unit Cost (£)	Quantity/Length	Total (£)
Shared USSD code. Issued by African Talking Limited for Nigerian MNOs	Setup	10	Two weeks	20

Hosting on Heroku	Monthly	5	Two months	10
Domain	Monthly	5	Two months	10
Miscellaneous (10% of costs)				4
			Total	**44**