International Journal of Finance and Banking Research
2023; 9(2): 30-38
http://www.sciencepublishinggroup.com/j/ijfbr
doi: 10.11648/j.ijfbr.20230902.12
ISSN: 2472-226X (Print); ISSN: 2472-2278 (Online)

Enhancing Mobile Banking Security through Blockchain Technology: Mitigating Unauthorized Access and Protecting Financial Assets

Ernest Aryee

School of Technology, Ghana Institute of Management and Public Administration (GIMPA), Accra, Ghana

Email address:
ernestaryee11@gmail.com

To cite this article:
Ernest Aryee. Enhancing Mobile Banking Security through Blockchain Technology: Mitigating Unauthorized Access and Protecting Financial Assets. *International Journal of Finance and Banking Research.* Vol. 9, No. 2, 2023, pp. 30-38. doi: 10.11648/j.ijfbr.20230902.12

Received: May 8, 2023; **Accepted**: June 1, 2023; **Published**: June 15, 2023

Abstract: Mobile banking has revolutionized the way individuals access financial services, providing convenience and accessibility through mobile devices. However, the increasing prevalence of mobile malware and security threats has raised concerns about the safety of mobile banking platforms. This study proposes a solution to enhance the security of mobile banking by leveraging blockchain technology and implementing various security features. Through a qualitative research approach, the study emphasizes the need to address cybercrime and fraudulent activities in mobile banking. The proposed solution includes measures such as authentication, authorization, data confidentiality, secure data cleanup, prevention of data transfer, device integrity checks, and encryption. These measures aim to strengthen security, protect against intrusions, and reduce fraudulent activities. Additionally, the solution offers a customizable and user-friendly mobile app that banks can adapt to meet their customers' needs. By incorporating blockchain technology and preventive measures, the proposed solution aims to increase user trust and confidence in mobile banking. This research contributes to understanding mobile banking security issues and provides practical recommendations for addressing these concerns. It lays the groundwork for future research and development in the field, highlighting the importance of proactive measures and staying updated with evolving technologies and threats.

Keywords: Digital Financial Services, Mobile Banking, Blockchain Technology, Malware

1. Introduction

1.1. Research Background

Digital financial services (DFS) render access to formal financial instruments through mobile technology which is considered a rapidly growing industry. Telecommunication industries, banks and 3rd party software companies manage mobile money networks on which these DFS operate on. One critical aspect is that services like this offer people with no formal financial history to establish an account most likely not needing to go long distances or travel to a physical bank. [2]

Mobile Banking provides features such as checking mini statements and account history; account activity alerts, access to card statements, mutual funds, equity statements, bill payment processing, pension plan management, access to card statements, status on cheques, stop payment on cheque, ordering checkbooks, insurance policy management, monitoring of term deposits, balance checking in the account, PIN provision, change of PIN and reminder over the internet, domestic and international fund transfer, recent transactions, due date of payment, micro-payment handling, mobile recharging, commercial payment processing, peer to peer payments and deposit at banking agent. Text messages are being received by customers which is allowed by Mobile Banking showing their account balance. It has been asserted that mobile banking has spread around the world, and it has brought about positive change from the customer's perception, could this be concluded about Ghana as well? [3]

Unfortunately, mobile malware is quickly increasing in frequency and sophistication in the past few years and has caused a variety of damages including the leaking of sensitive financial data, financial loss, and identity theft. In particular, the attention of many cybercriminals has been attracted by mobile banking apps. There are a lot of disquietude with the security aspect of mobile banking since

mobile devices are vulnerable to threats, attack, and loss. [4]

Some activities that put mobile banking at risk are when a customer accesses account on a public or unsecured Wi-Fi networks, when during accessing account there happens to be a reception drop which invites the probability that there could be a misfire with the data contained in your banking transaction which could be intercepted by an unauthorized third party and also sharing phone or companies computers can give unauthorized people access to sensitive credentials like your account passwords and others that can make them breach the system causing a loss to the bank or mobile banking service provider.

Proposed solutions to counter such activities stated above were training staff to identify customers at higher risk and provide adequate advise on risk, use sustained communication campaigns to raise or increase awareness warning customers about con schemes and other financial crime risks, Share experience and exchange information about the account mules within the industry and other stakeholders, Current efforts clearly lack structure, coordination and consistency, Tight IT Security policy and management framework. [6]

Why do mobile banking security issues exist despite these solutions? How safe is our money on these mobile accounts? What can be used to address these accesses by unauthorized personnel?

In an effort to deter the increasing threat this study seeks to find solutions to these questions by developing new practices, techniques and incorporate blockchain technology to lessen the security risks associated with mobile banking.

1.2. Research Problem

A well-connected financial system is imperative to a country's economy, not only for facilitating economic transactions for the community as a whole but also to serve as a vehicle for savings and long-term planning at the individual level. However, many low-income countries, especially in the rural regions, do not have access to formal financial institutions for lack of infrastructure, funding and oversight capabilities. It is reported that 2.2 billion people in the world do not have access to a traditional bank account. Digital Financial Services- the use of technological financials solutions including but not limited to mobile money can be enabled to engage this portion of the population and provide formal financial services to the unbanked. [8]

Mobile banking technology has been adopted by commercial banks as a strategic tool for market penetration without massive investment in physical infrastructure. The technology has been very instrumental in serving a wide and ever-growing customer base with fast, efficient, and convenient quality services. [5]

However, the rise of fraud and other security attacks have raised questions about the security of these mobile banking platforms. In the field of Mobile money, which is a subset of mobile banking, as in March 2015, there were 31,154,420 subscribers which use mobile money platforms by the various major telecom industries which are Vodafone and MTN by National Communications Authority in 2015. But unscrupulous persons continue to use mobile money services as a conduit to scam others. The sustainability of the service is being threatened by these fraudsters, who when left unchecked can bring abrupt end to the operations. The relatively high mobile money fraud rates recorded are hard to trace and devices and legislations available on the mobile money operations are lax to apprehend the perpetrators. This is a salient economic problem but a careful review of previous literature indicates that little on fraudulent transactions on mobile money services have been captured in the literature. This can be attributed to inappropriate fraud indicators to detect, measure, and prevent the menace. [1]

The need for a technological system to reduce or mar out these security breaches or issues is necessary. Technological innovation is often regarded as the primary driver of long-term economic growth, and the place of innovation has arguably never been faster. A technology such as Blockchain is what this study seeks to propose as a solution to solve these security issues in mobile banking applications or sectors. At its heart, a blockchain is a data structure in which every modification of data is agreed to by participants on a network. Once a data modification has been agreed to, it is combined into a block with other modifications that have taken place within the same, short timeframe. This block is then appended to a chain of previously agreed upon blocks, creating a complete record of all data modifications that have ever taken place. Cryptography is used to ensure that previous data modifications are safe against tampering by any participant or minority of participants and that no new modifications can be made without detection. As a result, participants can trust the data held on a blockchain. [7]

It is in this light of the foregoing that this study sets out to unearth the potential of blockchain to solving mobile banking security issues.

1.3. Research Purpose

To suggest, design, develop and implement a blockchain technology-based solution to mobile banking security issues such as fraud or cyber-attack.

1.4. Research Objectives

To suggest a clear-eyed view of the potential of blockchain technology to help meet economic development goals by fixing mobile banking security issues.

To design the flow and structure of using the blockchain technology to solve the security issues in mobile banking, its strengths, and weaknesses.

To develop a mobile application system based on the blockchain technology partnered with a bank to offer safe and secure mobile banking services.

1.5. Research Significance

This study is arguably one of the best studies to solve the security issues of mobile banking. To date, the existing solutions haven't solved them, yet in this case this new research seeks to solve it. Though there might be few

blockades in the path currently, it can arguably be said that Blockchain holds the potential to change the finance and banking sector by reducing potential cost and labour saving if such security issues in their mobile banking aspect is solved. There are other numerous benefits to be enjoyed by mobile banking operators and their customers.

Reduction in settlement time where payments and remittance settlement can occur rapidly rendering people access to their capital when they need it, is a crucial benefit that can be enjoyed and a plus to the value of mobile banking. Also, time and cost efficiencies could support large amounts of small transactions or micro-transactions within a trusted network.

However, storing transactions in automatically shared tamper-proof databases would take away the need for complex procedures and clearinghouses and ensure that banks do have their records in sync, hence eliminating third parties from having easy access to information.

This study also seeks to bring on board that the blockchain in real-time can track transactions in decentralized systems with no double-spending or transactional repudiation. Blockchain could support smart contracts, transactions that include multiple assets, transactions that include multiple parties and two-way transactions. This will allow the unbanked not only access to bank accounts but access to global capital markets as well by providing all types of value transfers.

Interesting enough, Blockchain can cut operational costs which banks are targeting and reach the customers at the edge of wireless and not just bank accounts. A secure transaction ledger database will be shared in an established, distributed network.

Storing transactions in blockchain could eliminate the need for complicated procedures and clearinghouses, saving time, money and the risk of error. The allowance of frictionless savings and investments gives people more control over their financial destiny. Embedding business rules into contract using digital technology, including automated execution of contract terms and payments will simplify, complex procurement, negotiation, and verification processes. The effect of fixing mobile banking security with this technology could go a long way to affect other operations that are conducted in the country and that would increase the development rate of the country due to higher productivity. The lives of some individual are all the monies they have in these mobile bank, hence the need to rapidly solve this security threat is high, that's why this study be pursued further to save the lives of individuals and the mobile banking sector itself.

However, the blockchain technology not limited to only solving mobile banking securities can be used in different field such as the health industry, Agriculture Industry, Sporting and Art industry. The thoughts, ideas and structures this study reveals could be used as a stepping stone to innovate creative solutions to solve problems in the few mentioned fields above.

2. Literature Review

2.1. Overview of Mobile Banking Security

In this Chapter, the emphasis would be placed on the technical definition for Mobile Banking, the advantages of Mobile Banking, the disadvantages of Mobile Banking, the security issues faced by Mobile Banking.

Mobile Banking could be interpreted as the usage of mobile devices or phone to perform financial transactions linked to the respective client's account. [17]

Also, Mobile Banking is considered or looked at in the perspective of it been a mechanism that enables customers of a financial institution to undergo transactions using Mobile devices such as Smart Phones, Tablets / notebooks as a medium. [16]

Freedom of an estimated high degree is given to customers when they use mobile devices to access banking services, since not only does it give them charge over what they are doing it gives them the opportunity to do their banking independent of their geographical location and time and not to bother about opening and closing hours of a bank unlike the traditional banking.

Mobile Banking provides features such as checking mini statements and account history; account activity alerts, mutual funds, ordering checkbooks, equity statements, bill payment processing, access to card statements pension plan management, access to card statements, status on cheques, stop payment on cheque, etc. [3]

Security which for so long has been the concern of mobile banking. Banks are the ones responsible for providing all the needed security to protect the information exchange between them and their customers. The main objectives of security in mobile banking are to make sure application and data access are controlled, data transmission is secured, data integrity is protected and if there be any loss of device the impact should be limited, hence the wireless adaptation of PKI and TLS/SSL for mobile banking to tackle these objectives. However, cyber-attacks and other fraudulent activities are still threats to security.

2.2. Methodology for the Review

There was selection of articles from various databases such as Scrip, Research Gate, Semantic Scholar, Diva, Open access, Academia, KNUSTSpace, ijrms, scholar and Google at large. The keywords or search terms used are presented in Figure 1. There were limiters, where we delimited the search to only articles within the last 5 years which consisted of Article (Doc. Type), academic journals, full text articles, peer reviewed journals. In total, there were 50 articles downloaded based on all the search term combinations in Figure 1.

Using the various keywords and others which might have been recorded in the table, the Research Gate Database contained more than 200 articles, where only 3 were download due to constraints on the keywords. Scrip database recorded 1302 articles, but only 2 were download, Semantic Scholar had about 2,840 articles on Mobile Banking Adoption and the examination of security risk of mobile banking, but for our research purpose we download 2. Diva produced 51 articles on fraud detection, open access displayed 5904 articles, Academia showcased 2,662 articles, KNUSTSpace, the database or repository of one of the leading university schools in Ghana produced 2785 research topics on the impact

of mobile money, ijrsm database had more than 6018 articles, scholar contained about 31, 200 articles on the security of mobile banking Applications and Google which isn't a database but a connector of databases, it works such that it searches the keywords in various databases and displays the corresponding articles for download without me going personally to the database to search, brought out in total more than 89,000 articles where 37 articles were downloaded. And also has the highest number of downloads among the 10 various databases used in this research.

These 50 articles were schemed thoroughly, summarized and referenced in this study at their various respective topics. It is of no doubts that the articles downloaded are of good quality in terms of the information they hold and the knowledge gained when one reads it.

Database	Keywords	Total Search Results	Limiters	No. of articles download
Research Gate	Mobile Banking Fraud, M-Banking Security	More than 200	Default	3
Scrip.org	Mobile Banking, Mobile Banking Security	1302	Default	2
Semantic Scholar	Mobile Banking Adoption, Examining security risks of mobile banking	About 2,840	Last 5 years	2
Diva	Fraud Detection	51	Default	1
Openaccess.nhh.no	Research gaps for mobile services	5904	Default	1
Academia.edu	Mobile Banking services	2,662	Default	1
KNUSTSpace	Impact of Mobile Money	2785	Default	1
Ijrsm	Mobile banking and security challenges	More than 6018	Default	1
Scholar	Security of mobile banking Applications	About 31,200	Default	1
Google	"Mobile Banking security", "Fraud in mobile banking", "Mobile money transfer services", "background of mobile banking", digital financial services, blockchain technology for mobile banking	More than 89,000	2014 - 2019	37

Figure 1. *An image showing selection of articles from different databases.*

2.3. Dominant Issues in Mobile Banking Security

2.3.1. Security of Mobile Banking

The belief of insecurity has been the major undertaking of mobile banking technology and services adoption. According to Federal Reserve's survey, forty-eight percent (48 %) of respondents referred to their predominant reason for not using mobile banking as I'm concerned about mobile banking's security. Also, referring to the same study, respondents have been requested to rate the security of mobile banking for protecting their personal information or statistics and thirty-two percent rated it as somewhat unsafe, while 34% were not certain if it has a good security. These survey showcases a significant barrier to the use of mobile banking products and services. Only when the security is completely shielded, the mobile banking can undergo other traditional banking business activities, hence making security the foundation for the development of mobile banking. Frauds and other cyber-attacks which are threats to security can be preventive with simple measures like, activate your mobile device's code lock, turn off wireless connections when not needed, utilize solid phrase (password) to lock your cell phone, never share individual information with outsider, never store individual financial subtleties in mobile phones and while banking or shopping online, make sure the sites are https or shttp. Concluding, Precaution is the best way to keep up verified transactions in this mobile banking system. [16]

Mobile Banking is appealing in the light of the fact it is an advantageous way to perform remote banking, however the presence of security setbacks cannot be overlooked in the present mobile banking implementations. The wireless communication information security issues identified with mobile banking incorporate Information spillage, misfortune and mutilate. Because of the limited tools to protect the wireless transmit media, confidential banking information may be leaked, lost or misshape in the day to day transaction gadgets. This gives space for attackers to intercept and erase, include or alter certain vital information to damage the typical utilization of genuine users. Additionally, Virus Attacks are not to be left out, since virus could be utilized to destruct mobile phone functions and expel records and other data, hence making the potential dangers of mobile banking far more prominent than network banking. To fix these issues the idea of system and data integrity is indispensable, where mobile banking systems would be equipped or furnished with appropriate safety measures such as firewalls, intrusion detection system and fast

recuperation mechanism to ensure data security and integrity. Be that as it may, Digital Signature also assumes a vital role in the data authentication and non-denial. RSA algorithm and ECC algorithm are all structures used in the digital signature technology. Concluding, as the rapid pace of technological change continues, the list of all known vulnerabilities of the mobile channel should be maintained by a central organization and updated by experience, to which mobile financial provides and regulators would have the right to access as a baseline for their risk frameworks. [17]

2.3.2. Adoption of Mobile Banking

M-banking otherwise called Mobile Banking is an all-encompassing type of banking on the web, it gives brief reaction to clients, convenience or comfort, time autonomy and it is cost sparing. Banks have now been presented with this chance to increase consumer market through mobile services with these advantages. It would serve mobile banking services providers well to comprehend what impacts the aim to utilize or adapt m-banking innovations particularly among young adults who are probably going to be future adapters and users of mobile banking- a beneficial service to generate revenue from m-banking investments. The one of numerous reasons why mobile banking has not been widely acknowledged or embraced is as a result of the absence of trust in this service. An expansion in the utilization of smart phones will prompt an increment in the selection of m banking by most customers in the following couple of years. It has also been taken a gander at that the primary users of mobile banking are aged between 25 and 34 years old, who for the most part place extraordinary value on the effective use of time and also the fact that they have had experience with other mobile applications give them confidence or trust in the security in the mobile banking. It has been distinguished that the easy usability of mobile banking apps has a positive impact on perceived value and on the intentions of users to embrace or keep utilizing of mobile banking services. Finishing up, it is certain due to statistics that 57.7% of IT students would enjoy using wireless networks in their activities which would cause them adopt mobile banking services because it suits their technology driven way of life. Notwithstanding, authentication mechanism ought to be improved in mobile banking services to turn away fraudulent activity and ease fears of privacy issues all together that Trust may be increased, and hence m-banking appropriation rates increase. [10]

Albeit mobile banking is still anticipated to be a trend, some industry reports infer that mobile banking services don't have any genuine effect on bank profits, and this makes banks more progressively hesitant to receive mobile banking particularly in countries where other banking techniques or methods are well settled, or market is generally little. Also it was observed that the main reason for the lack of consumer interest for mobile banking is the apparent voice-driven nature of the mobile phone. Among the hindrances to mobile banking adoption, most authors quote security and protection issues, open doors for fraud, low speed (GSM), unreliability (GPRS), absence of norms, absence of expansion in services, lack of customer mindfulness, significant expense, and the pervasiveness of other banking methods. Therefore, it is accepted that the mass appropriation or adoption of mobile banking will rely upon the arrangement of secure, solid and simple to customize user interfaces which can be actualized on a multi-standard, multi-functional mobile device intended for a long life and rough help. [14]

2.3.3. Fraud Detection

From the beginning of time, there have been those who somehow try to circumvent established rules and in the world of finance this is no exception. One way to circumvent rules is to commit fraud which is explained as the criminal act with intention of obtaining financial or personal gain, where an example of achieving such intention in the sector of finance is termed money laundering. A fairly new problem within the world of finance is phishing, which has become more common since the Internet with E-commerce, online shopping, and the simplicity to do banking transactions online. Phishing and exploitation are mostly the two types of fraud in the virtual financial world where mobile banking is a subset of. In fraud detection there are two approaches the anomaly and signature detection. When detecting fraud by searching for anomalies the detection system searches for users with a behavior that does not comply with the normal behavior of the majority of users. Signature-based systems looked for certain patterns that are predefined by fraud in the sense that as long as a user does not follow any of the patterns for a specific signature of fraud the user we classify no fraudulent user otherwise the user will be identified as a fraudster. Concluding, it has experimented that it is possible to combine the quantile-statistics together with Benford's law, the law of digits' distribution, to find fraud in data from logs within Digital Financial Services. [12]

2.4. Gaps for Future Research

Based on reviewing of other literatures or research topics, several paths have been seen for future research on mobile banking and other digital financial systems.

It has been identified that Mobile Banking is here to stay and also mobile devices are a technology that can possibly change the substance of retail banking. In the future, there are desires to see a shift from OS-Specific applications to browser-based application because right now applications are developed and launched focusing or targeting at the various operating system iOS and Android for the most part.

According to [15] Mobile Money a digital financial service has the greater probability of stimulating the economic growth and improving billions of lives across the world, therefore suggests that future research should be done to find out the effect of network stability in improving mobile money technology services and any other area to improve digital financial systems.

Also, it was identified that most literatures were dominant on that adoption of mobile services therefore it would be interesting if for future research there would be digging into the possible effects of mobile services in terms of influence and effects of using mobile apps. [13]

Future Research work should be done on how to secure mobile banking apps code from the ground up with encryption,

how to secure the network connection from the back end, how to develop a strategy to put in place a solid API security, How to utilize behavior analysis of a real time text and email alerts and how to add tight multifactor authentication feature in other to prevent fraudulent activities in mobile banking. [11]

Planning for the future to research in the way to utilize workflow technology to simulate mobile banking security dangers, for example, how to mimic the attack on mobile check deposit so that we can even more likely increment the security familiarity with mobile banking application. We are also keen on considering the use of biometric mechanism in mobile banking applications and the harmony between security and usability or convenience for mobile banking applications. [4]

The use of Blockchain technology can dispose off the requirement for muddled techniques and clearinghouses, spare time, cash, the danger of mistake and in whole due to its secured and encrypted structure unauthorized personnel such as hackers who are identified for causing fraudulent attacks would find it very difficult to cause havoc hence to deter them from attacking mobile banking systems. Despite these, there are some few unsettled doubts about blockchain where future researches should be based on. The first has to do with the uncertain regulatory status, where due to the decentralized nature of blockchain, if the government regulation status stays agitated, the technology would confront an obstacle in far adoption by financial institutions. Also, even though private or permissioned blockchain and solid encryption exist, there are still some cyber security concerns (i.e.: the internet is not 100% safe and there is no technology that cannot be broken into, etc.) that need to be addressed.

2.5. Literature Review Summary

This chapter brought to light the overview of Mobile Banking Security, where key variables like mobile banking and mobile banking security was elaborated, the impact or advantages and disadvantages of mobile banking and some of the security issues faced by mobile banking despite the use TSL/DLL technologies to combat security in mobile banking.

The study went further to showcase the dominant issues in the area of mobile banking security, we had three main themes.

Firstly, the security of Mobile Banking. Most researchers had their researches on this field exposing the security issues in mobile banking, the current methods or technologies used for security in mobile banking and the impact of bad security on mobile banking. All these have yielded much understanding and knowledge of security of mobile banking which have been incorporated in these studies to help find a better solution to fix and enhance the security of Mobile Banking for economic growth and widely national development.

Secondly, Adoption of Mobile Banking. The perception of people towards digital technology and their appreciation to adopt a digital financial technology like mobile banking was tackled under this theme. There have been surveys conducted in research under this theme that has made it certain to say that the only reason why one would fear to adopt to mobile banking is the uncertainty about the security of the applications used in the servicing.

Lastly, Fraud Detection has been the concern for most researchers hence much researches on such area. More education was done on the examples of fraudulent activities and the various detection methods used to detect fraud such as the combination of quantile-statistics and Benford's law, etc.

However, not all the researchers were able to solve all the security issues in mobile banking, hence the room to discuss future researches that would help to fully combat all the security issues. And that was vividly explained in 2.4.

3. Research Methodology

The process of applying various techniques known to for collection and analyzing of data in a field of study is what is termed Research Methodology. This study implemented a qualitative research approach to gain insights on the perception of individuals about the security of Mobile Banking.

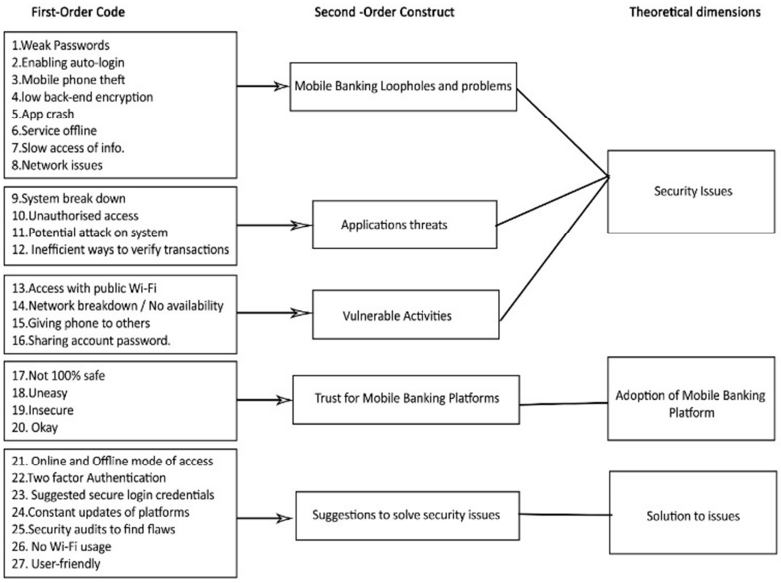

Figure 2. *Structure of a qualitative research approach to gain insights on the perception of individuals about the security of Mobile Banking.*

3.1. Research Design

3.1.1. Awareness of the Problem

In late news broadcasted on various media channels, the rise of cyber-crime and other fraudulent activities had been the discussion and therefore placing heat on the government and all technological firms to investigate and find out the reasons for such activities and find best ways to reduce or bring such disturbing activities to an end. On this basis, the author of this study then saw it wise to play a role in solving this problem. After some researches to find out how these cybercrime fraudsters are able to commit such activities, the author found out some reasons and by means of questionnaires, data was gathered to verify if people really commit such activities hence giving the intruders chance into their mobile banking systems to cause harm to their accounts and also to gather their perceptions about the security issues of mobile banking. Below is a qualitative data structure on this research.

3.1.2. Suggestion

From the data gathered, a viable solution can be found to reduce the rate at which intruders can harm the mobile banking platforms. Building a mobile app based on a recent technology called blockchain which would enhance the back-end encryption of the data and account details, such that intruders would find it difficult to actively harm system without been traced, due to decentralization, transparency and immutability of the blockchain technology or framework. Other features that the app seeks to provide is online mode of accessing the platform, implementation of 2 factor authentication, provision of suggestive login credentials to reduce the use of weak passwords and constant inhouse updates and security audits to find flaws and fix them. Also, the platforms wouldn't allow usage of Wi-Fi networks, also above all the apps would be simple and user-friendly.

3.1.3. Design

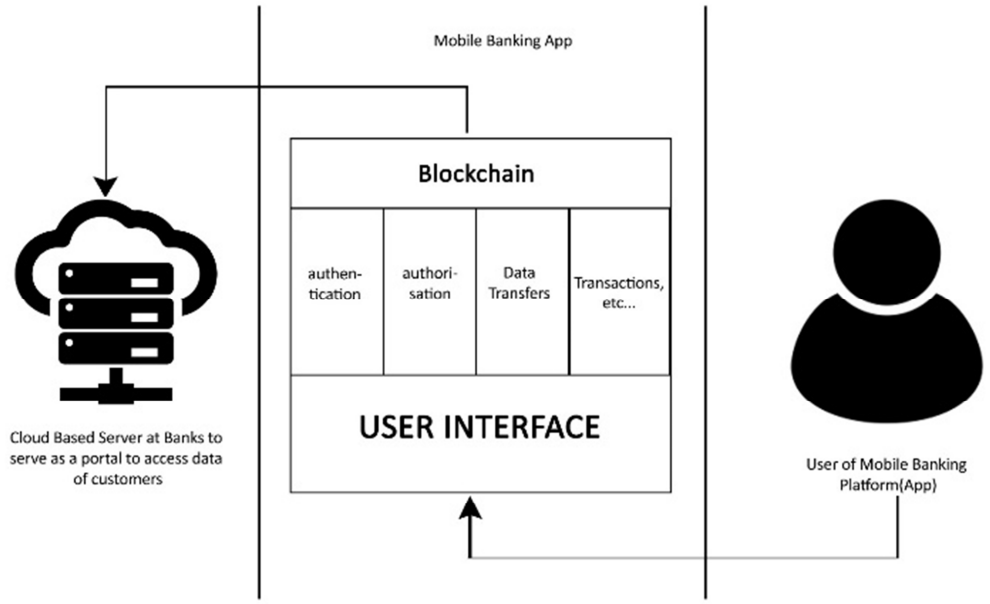

Figure 3. *Design representation of the mobile banking app.*

3.1.4. Development

Building of this artefact is to be done in phases, from the authentication to the data encryption. Details on each phase would be explicitly explained for easy implementation by future researches. Recommendations from [18] would be used in building the platform. Below are the faces and the way to work around them.

Authentication: For user ID plus password and the double factor authentication, a secured XML-based framework would be used. Also, for additional security the user location would be checked using GPS during the authentication process.

Authorization: After the authentication, the back-end services would be checked to verify if the user has the required access to the system and then display the necessary navigations for the user to use.

Data Confidentiality: Because of the fact that the system must not store any sensitive data on the file system and also for sensitive information not to be leaked through logs and error messages, a tool called Dexguard and Arxon's EnsureIT for Android and iOS respectively would be used.

Secure Data Cleanup and Data Transfer Prevention: When a user log – off, all data requests, account data and user-related information would be securely wiped. And in the case where there is any sign of tempering of application, the application would be forced to shut down. Also, all data from the clipboard would be removed so it can't be transferred outside the application.

Jail – Break / Rooted Device Check: When a device is rooted or jail-broken, hackers can easily find their way

through the system, therefore the app must be able to prevent the hackers from accessing it, therefore the use of Trusteer Mobile SDK would be best to verify if the phone is rooted and sends scores to the app to determine if the app should be closed or the score should be sent to the very back-end of the system over a secured channel for further investigations.

Anti – Debugging Mechanism: The application would be able to prevent debuggers from reading sensitive data from memory in use by another running application. The use of Dexguard / EnsureIT would be used to support the removal of logging data, debug or test codes.

Blacklisting Older Versions of the App: In case of any security breach, older versions of the app can be blocked on the back-end server.

Anti – pharming protection: Prevention of the reduction of traffic that would occur to a malicious server would be a key in-built feature and hat would be done by checking that the host-name look-up with DNS resolves to a white- listed IP in the back-end server.

Connection and Asset Encryption: Encryption of networks and asset files transparently and hiding of important data would be resolved with the blockchain framework.

3.1.5. Implementation

The Mobile App would be a customized one, in the sense that it can be modified by any bank to suits the need of the customers, but the security features would still be intact. Users can have access to the app after customization by the banks on both Google Play store and Apple play store or any verified download site, based on the architecture of the user's device. Due to the decentralized nature of the blockchain framework, a secured portal would be built to give the bank access to necessary data of their customers.

3.2. Research Methodology Summary

This study has explicitly brought to light the reasons behind the in-depth passion to pursue this research in 3.1.1. In 3.1.2, the suggested solution and features of the solution has been expounded in there. The qualitative data structure has been shown in 3.1.3 to help have a good view at the angle with which this research has been tackled. Incorporation of the first-order codes, second-order codes and theoretical dimensions make it easy to understand the broad view of the security issues of Mobile Banking.

The development phase in 3.1.4, holds the tactical and technical methods to ensure the security of the mobile app and its relations. And finally, this research tackled how the solution is going to be implemented in 3.1.5 to help reduce the fraudulent activities that have been on the rise on mobile banking platforms.

4. Result and Discussion

The implementation of a qualitative research approach allowed for insights into the perceptions of individuals regarding the security of Mobile Banking. Through questionnaires and data collection, the study aimed to verify if people engage in activities that give intruders access to their mobile banking systems, thus causing harm to their accounts. Additionally, the study gathered information on individuals' perceptions of mobile banking security.

The gathered data revealed several key findings. Firstly, it highlighted the rise of cybercrime and fraudulent activities as a significant concern in society. The media's coverage of these issues had prompted government agencies and technological firms to investigate and find effective solutions. This study recognized the importance of addressing these problems and aimed to play a role in providing a viable solution.

Based on the data analysis, the study proposed the development of a mobile app utilizing blockchain technology to enhance the back-end encryption of data and account details. The use of blockchain technology ensures decentralization, transparency, and immutability, making it difficult for intruders to harm the system without being traced. The app also incorporates additional security features such as online mode access, two-factor authentication, suggestive login credentials to discourage weak passwords, and regular in-house updates and security audits to identify and address vulnerabilities. Moreover, the app restricts the usage of Wi-Fi networks to enhance security.

The discussion delved into the design and development phases of the proposed solution. The authentication process involves using a secured XML-based framework, along with GPS-based user location verification. Authorization checks ensure that users have the required access to the system before displaying the necessary navigations. To maintain data confidentiality, the system avoids storing sensitive data on the file system and uses tools like Dexguard and Arxon's EnsureIT for Android and iOS, respectively. Secure data cleanup and prevention of data transfer are also prioritized to ensure that user-related information is securely wiped and inaccessible after logging off. The app incorporates measures to detect and prevent access from jailbroken or rooted devices. Anti-debugging mechanisms are implemented to protect sensitive data from being read by debuggers. Older versions of the app can be blacklisted on the back-end server in case of security breaches. Anti-pharming protection is provided by verifying that the host-name lookup with DNS resolves to a white-listed IP. Connection and asset encryption are achieved through the use of the blockchain framework.

In the implementation phase, the mobile app is customized to meet the specific needs of different banks while maintaining the security features. The app can be accessed through authorized download sites such as Google Play Store and Apple Play Store, or any verified download site based on the user's device architecture. The decentralized nature of the blockchain framework necessitates the creation of a secured portal to provide banks with access to necessary customer data.

5. Conclusion

In conclusion, this study aimed to address the security issues associated with mobile banking by implementing a

qualitative research approach. The findings highlighted the importance of addressing the rise of cybercrime and fraudulent activities. Through the use of blockchain technology and various security features, a viable solution was proposed to enhance the security of mobile banking platforms. The implementation of the solution involved phases such as authentication, authorization, data confidentiality, secure data cleanup, prevention of data transfer, jailbreak/rooted device checks, anti-debugging mechanisms, blacklisting older app versions, anti-pharming protection, and connection and asset encryption.

The proposed solution offers a robust and user-friendly mobile app that can be customized by individual banks to suit their customers' needs. The app provides enhanced security measures to protect against intrusions and fraudulent activities. By incorporating the blockchain framework, data encryption, and other preventive measures, the app aims to reduce the occurrence of fraudulent activities in mobile banking.

Overall, this research contributes to the understanding of security issues in mobile banking and offers practical recommendations for addressing these concerns. It provides a foundation for future research and developments in mobile banking security, emphasizing the importance of staying proactive and up to date with evolving technologies and threats. The proposed solution has the potential to make mobile banking platforms more secure, thereby increasing users' trust and confidence in conducting financial transactions through mobile devices.

References

[1] Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., & Dwomoh-Okudzeto, Y. (2019). Control of fraud on mobile money services in Ghana: an exploratory study. Journal of Money Laundering Control, 22 (2), 300–317. https://doi.org/10.1108/JMLC-03-2018-0023

[2] Castle, S., Pervaiz, F., Weld, G., Roesner, F., & Anderson, R. (2016). Let's talk about money: Evaluating the security challenges of mobile money in the developing world. Proceedings of the 7th Annual Symposium on Computing for Development, ACM DEV-7 2016, 1–11. https://doi.org/10.1145/3001913.3001919

[3] Cudjoe, A. G., Anim, P. A., & Tetteh Nyanyofio, J. G. N. (2015). Determinants of Mobile Banking Adoption in the Ghanaian Banking Industry: A Case of Access Bank Ghana Limited. Journal of Computer and Communications, 03 (02), 1–19. https://doi.org/10.4236/jcc.2015.32001

[4] He, W., Tian, X., & Shen, J. (2015). Examining the security risks of mobile banking applications through blog mining. CEUR Workshop Proceedings, 1353 (January 2015), 103–108.

[5] Karanja, J. (2017). INVESTIGATION INTO THE RISKS FACING MOBILE BANKING: A CASE OF COMMERCIAL BANKS IN KENYA. SPRING, 200.

[6] Omuga, S., & Phone, C. F. E. (2014). Mobile money fraud. (0721291705), 1–16.

[7] Pisa, M., & Juden, M. (2017). Blockchain and Economic Development: Hype vs. Reality. Center for Global Development, (July), 150. Retrieved from https://www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf

[8] Yu, S., & Ibtasam, S. (2018). A qualitative exploration of mobile money in Ghana. Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies, COMPASS 2018. https://doi.org/10.1145/3209811.3209863

[9] Lyte, B. (2015, March 27). WiseBread. Retrieved from 5 Dangers of Mobile Banking — And How to Avoid Them: https://www.wisebread.com/5-dangers-of-mobile-banking-and-how-to-avoid-them

[10] Govender, I., & Sihlali, W. (2014). A study of mobile banking adoption among university students using an extended TAM. Mediterranean Journal of Social Sciences, 5 (7), 451–459. https://doi.org/10.5901/mjss.2014.v5n7p451

[11] Joshi, D. K. P. (2018). A Comprehensive Study of Vulnerability Assessment Techniques of Existing Banking Apps. International Journal for Research in Applied Science and Engineering Technology, 6 (4), 967–972. https://doi.org/10.22214/ijraset.2018.4164

[12] Kappelin, F., & Rudvall, J. (2015). Fraud Detection within Mobile Money. A mathematical statistics approach. 54. Retrieved from http://www.diva-portal.org/smash/get/diva2:865559/FULLTEXT02.pdf

[13] Nysveen, H., Pedersen, P. E., & Skard, S. E. R. (2015). A review of mobile services research: Research gaps and suggestions for future research on mobile apps. SNF Working Paper No 01/15. 1–74.

[14] Petrova, K. (2002). Mobile Banking : Background, Services and Adoption. International Marketing, Management & Consulting.

[15] SALIU, I. (2015). Assessing the Impact of Mobile Money Transfer Service on the Socioeconomic Status of the Mobile Money Vendors : (August).

[16] Sasikumar, G. (2017). Mobile Banking and Security Challenges. International Journal of Scientific Research and Management, 5 (07), 6014–6018. https://doi.org/10.18535/ijsrm/v5i7.26

[17] Szczepanik, M., & Jóźwiak, I. (2018). Security of mobile banking applications. Advances in Intelligent Systems and Computing, 635 (July), 412–419. https://doi.org/10.1007/978-3-319-64474-5_35

[18] Tank, A., Desai, C., & Technology Solutions, C. (2014). Mobile Banking Security: Challenges, Solutions. Cognizant, (July), 1–5. Retrieved from https://www.cognizant.com/InsightsWhitepapers/Mobile-Banking-Security-Challenges-Solutions-codex898.pdf