Journal of Information Technology & Software Engineering
ISSN: 2165-7866
OPEN ACCESS Freely available online
Review Article

A Proposed Approach to Enhance User PIN in the Mobile Money Ecosystem

Afful Ekow Kelly*, Sellappan Palaniappan

Department of Information Technology, School of Science and Engineering, Malaysia University of Science and Technology, Selangor, Malaysia

ABSTRACT

The use of only numeric numbers as the base for the USSD PIN rather than alphanumeric was one of the security risks in the USSD mobile money services. The use of only a numeric key for PIN was far more convenient for users, but it also made them more vulnerable to attacks. The standard PIN length in the current USSD mobile money application was four numeric keys. The indication was that the PIN length was too simple for a simple system to break through. The study included 57 participants to uncover the vulnerability of users' PINs in mobile money services. The study proposes a two-in-one solution in which mobile money users can increase their PIN to six characters, and include alphanumeric keys. The current study will help to reduce the increasing threat of mobile money fraud in the FinTech industry.

Keywords: Mobile security; Personal identification number; Mobile money; Unstructured supplementary service data; SMS threat

INTRODUCTION

The security threat of mobile is very broad; as a result, the focus of the research is considered from the perspective of the general operation of mobile money banking. The general operation of mobile banking is two phases; thus, the bank or the telcos and the handset are used by the mobile user in their mobile money banking operations.

The direct interaction between the telecoms and handset is by use of a web portal and Short Message Service (SMS), where SMS is through Unstructured Supplementary Service Data (USSD) however, the SMS is the most common medium. SMS usage has grown in almost every sector of human development, from health care, e-government, education, agriculture, railways, mobile banking, and news alert to send reminders. These messages also include passwords and private information of user; in 2018, more than 9.1 trillion SMS were sent across the globe, constituting $1trillion in commercial value [1-5].

The use of mobile money has become very important in bridging the most critical services that also occurred during the COVID-19 pandemic. The role of mobile money became a saviour in the financial sector during a pandemic of this magnitude.

However, the importance of the usage of USSD for mobile money should not elude stakeholders from overlooking the emerging security threats associated to mobile money services. It is on this score that the research through more light on the weakness of the current user PIN used in the mobile money service and sought to introduce an alphanumeric PIN instead of four numeric PIN.

LITERATURE REVIEW

The review considers the structures associated with mobile money applications, as well as the security risk posed by USSD structures linked to mobile money services.

Mobile application

In designing mobile applications, there are a few other issues to solve, including simplicity of the application, user friendly, security, and a well established application referred to as a “killer application”. According to Hillman and Neustaedter, mobile application development is simply by virtue of whether such regulatory approval potentially makes service providers more reliable with their mobile application services [6-10]. However, according to Sarkar, et al., users would be discouraged from establishing flow if mobile applications have many difficulties.

Correspondence to: Afful Ekow Kelly, Department of Information Technology, School of Science and Engineering, Malaysia University of Science and Technology, Selangor, Malaysia, Tel: 233245000000; E-mail: affulekowkelly@yahoo.com

Received: 08-Oct-2022, Manuscript No. JITSE-22-18834; **Editor assigned:** 10-Oct-2023, PreQC No. JITSE-22-18834 (PQ); **Reviewed:** 24-Oct-2023, QC No. JITSE-22-18834; **Revised:** 10-May-2023, Manuscript No. JITSE-22-18834 (R); **Published:** 17-May-2023, DOI: 10.35248/2165-7866.23.13.331

Citation: Kelly AE, Palaniappan S (2023) A Proposed Approach to Enhance User PIN in the Mobile Money Ecosystem. J Inform Tech Softw Eng. 13:331.

Mobile device architects must thoroughly examine the application's environment. Therefore, designing mobile applications thoroughly to satisfy the needs of target users is highly significant [11-13].

Mobile application issues

This study classified the issues confronting mobile payment as; security, cost, standardization, convenience, technology and system quality. The fundamental taste of users to adopt technology varies. However, Dahlberg and Mallat indicate that the focus should be on safety and affordability to get customers to embrace the new payment system. The challenges in mobile money applications, and any solutions proposed must attempt to address them [14,15].

Standardization: Several academics suggest that the unavailability of the uniform approach poses apparent issues in the advancement of mobile payment services to attract users. According to MeT, the usage of mobile banking current market is characteristic of either an emerging thing, first with a plethora of concepts and indeed ideas, which might or might not be interoperable. Also, with a standard interface since the shared knowledge and convenience of use are vital, in the entire customer's delight is getting a service that meets their requirement and service deployment at ease. Finally, one of the most pressing issues in mobile payments is a lack of standardization, exacerbated by the mobile market's proliferation (Figure 1).

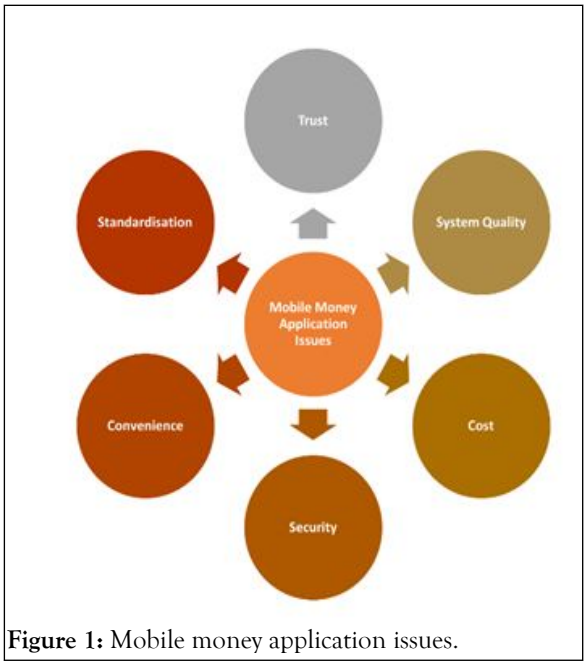

Figure 1: Mobile money application issues.

Trust: Trust in mobile payment services is mostly limited to the devices, applications, operators, regulations, and network infrastructure [16]. Trust encapsulates the fact that the user strongly expects that the data and transaction information that the operators and the banks primarily handle are not misused or trade off but is kept safe. This could be done when all the players put in appropriate measures to ensure and assume the trust needed [17,18].

System quality: Consumers obtain good impressions and adoption when they see that the service offers them is of good quality Zhu, et al. A difficult to use system has a low "perceived ease of use".

The strength of third party trustees, the crucial cryptography infrastructure to check secure transactions and the safeguard of privacy is an unquestionably crucial aspect in creating consumer adoption.

According to Corbitt, et al., when customers find inadequate integrity it may hinder their interest to use. However, system quality should primarily put into perspective the user's demand to understand how it will ease their response to service demand.

Convenience: Convenience and ease of use are both significant factors incentivizing all technological advancements. Mobile user views of mobile payment convenience have a favorable impact on the acceptance of "mobile payment services". Consequently, the accessibility of mobile payment systems is one of the reasons behind their popularity. However, in this age of rising hacking and cyber fraud, mobile money transactions come with the risk of financial and data loss. Compared to traditional financial service providers, the perceived benefit of the desire to use mobile payment is an appropriate basis to attribute the perceived usefulness of the intention to adopt mobile financial services. According to Liu, et al., although mobile payment is convenient, it also introduces dozens of new payment security concerns, leading to our subsequent discussion on security.

Security: Security knowledge, privacy issues, and trust problems are all possible causes of factors to disrupt the gains made in mobile commerce. Thus "mobile commerce started with the establishment of cellphones equipped with advanced cards", which provide security features not accessible through all the other e-commerce methods. The cell phone, with an embedded SIM card, seems to be an ideal recipient for a Public Key Infrastructure (PKI) system's secret key electronic signature.

However, this advancement is only possible if a tremendous amount of data security is ensured for the user's information and secured transactions. According to Gao, et al., the rising "adoption of mobile devices, as well as the development of digital systems" and applications, necessitates a human centered approach to mobile data security [19].

Privacy is a fundamental consumer prerogative, as users must not divulge their identity to other parties unless they are ready to provide that privilege.

Cost: Another factor that keeps surfacing in the face of adopting mobile payment is the transaction cost associated with the services provided, and related charges have not been uneasy. This is supported by Abooleet et al., most of these payment methods continue to face opposition due to a variety of factors, such as transaction costs. The acceptability of mobile money payment is completely dependent on those willing to pay the extra cost. It is, of course, not simple to convince clients to give more charges without good offerings. Operational expenses include both fixed but also payment system expenses, as well as user expenditures and technological infrastructure.

Security threats in SMS

Information security is the act of protecting information systems from unauthorized access for using any other than its original purpose. The distribution of SMS *via* a GSM system is not secured and is vulnerable to unauthorized access [20].

Common threats in SMS

The nature of the attack in a network system can be placed into two forms, thus internal and external; these attacks could also be referred to as active and passive respectively. We look closely at the specific attacks related to networks from which SMS is the predominant sector in its transactions.

Man-in-middle attack: This happens when the user is falsely authenticated by the use of a false network system. Before any message or call gets through, the user has to be verified; this is where the attack happens, the man-in-middle turn to use a "false BTS which uses the same network code of the subscriber" which makes it difficult to notice of the false authentication, as a result, turns to impersonate or commit any crime on the network.

Replay attack: With a replay attack, the perpetrator uses the old messages between the user and network to carry out such attacks. The user turns to trust the source and is ready to do anything such inquest this new message seeks to achieve.

Spamming: These are SMS messages which are sent as a nuisance or for an attack such as phishing or pharming. Several social marketers online turn to use SMS messages as a very legitimate marketing tool. But these turn out to be an inconvenience in some cases.

Denial of Service (DoS) attacks: This happens when bulk and repeated SMS messages are sent to a target mobile phone user, with the primary intention to deny the user the use of their phone.

SMS phishing: This uses the weakness in the SMS to send unsolicited information to a user with the main intention to cause harm.

Message disclosure: SMS by default is not encrypted; the user's message is temporarily stored in SMSC as plain text. This makes the SMSC center venerable to an attack, as such messages are intercepted either deliberately by a brute force attack. The information gotten could be used for a purpose which is not intended by the user. In some instances, the information could be of no use but viewed by a third party (Figure 2).

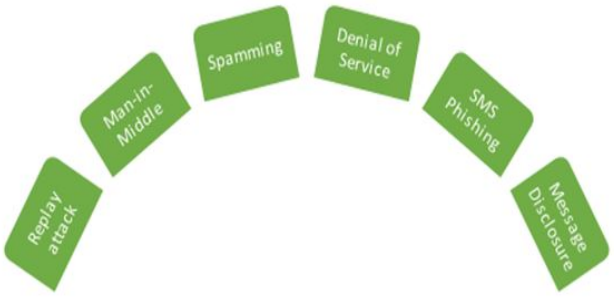

Figure 2: SMS threats.

The research organized a focus group discussion and engaged a group of users to give insight into the PIN composition of their mobile money usage. The outlook from those two discussions shows the nature of PIN created. This revealed the weakness of the user PIN and how easily a third party through social engineering and social media can get access to the user PIN. Out of 57 participants who took part in the study, Table 1 shows the outcome of respondents' pattern of choosing and creating their PIN. The participants were asked to change their PIN after the discussion.

Table 1: Pattern of PIN used by users.

Key	Digit of phone numbers		Year of birth		Others	
M-Male	15		23		19	
F-Female	F (9)	M (6)	F (15)	M (8)	F (6)	M (13)

The scenario in Figure 3 enforces the kind of PIN used and its lengths, this is easier and simple for the user. However, it unveils how vulnerable it is to access another user's PIN.

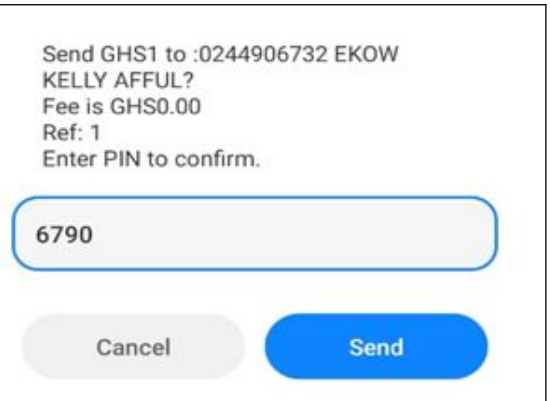

Figure 3: Length of PIN.

Application development tools

The service tools used for the development of the mobile money application, first, a local host server was created to expose the codes to the internet and Africa talk as simulation platforms. The study adopted Apache HTTP server as the internal server host. Also, ngrok was used to help tunnel the service of the webserver (Apache). For, the webserver and ngrok not to delay in the kind of service it is rendering a callback or web hook is used to support the flow of data access, this serves as stationery to where the webserver and external host can easily and continuously fetches its data for their use as and when it is needed.

Proposed user PIN solution for USSD mobile money service

The number of characters used as PIN authentication general determines the PIN's strength. Using "mobile money" services as a case, all the telecom operators' PINs are limited to only four (4) numeric characters. This makes it easier for anyone mindful of accessing another user's PIN with minimum brute force attack or shoulder looking to get hold of an individual PIN quickly. In contrast, with that comes a gap this study would want to fill in the current security arrangement by the operator of the telecom of mobile money in Ghana.

This demonstrated that the PIN length could be broken in less than an hour using simple computer algorithms in a brute force attack. The current size of the PIN stack was set to four for convenience and user friendliness, with little thought given to the threat such a length could pose in financial transactions involving mobile money banking. This resulted in users not making any conscious effort to create PINs that were difficult to guess. In any case, given the length of available keys, users simply used any patterns that were as convenient to them, such as the last four digits of their current phone number or their year of birth, as was discussed earlier. As a result, the research implementation in order to increase the length of the PIN key was successful. This was increased to six characters on the basis that if a user loses or misplaces their phone, they will have a much greater window of opportunity to report it to the appropriate telecommunications operators. The latter will then block access to the phone to be used by the default new owner. As a result, it is a win-win situation for both telecoms and users (Figure 4).

```
class Accounts(db.Model):
    id = db.Column('account_id', db.Integer, primary_key=True)
    name = db.Column(db.String(50)) # user input
    phone = db.Column(db.String(15)) # user input or from ussd_session
    email = db.Column(db.String(100)) # user input
    pin = db.Column(db.String(6)) # user input
    bank = db.Column(db.String(100)) #user input
    account_number = db.Column(db.String(30)) #user input
    bank_branch = db.Column(db.String(50)) #user input
    balance = db.Column(db.String(200)) # default 0, user input (teller)
    retry_chances = db.Column(db.Integer) # default 3
    creation_date = db.Column(db.String(10)) # progam generated
```

Figure 4: Programing code for user PIN keys.

The coding to increase the length to six characters from the current designated of four numbers. This introduction gives users the freedom to use any key combination of up to six characters, thus alphanumeric characters instead of only numeric. This is not to say that users can't continue to use the year of birth and other patterns discussed previously. However, users can add any additional characters to their existing keys. This makes the user's PIN length longer, and it a little more difficult to brute-force attack the user's financial account on the mobile money platform. Figure 5 shows what the mobile money interface looks when a user enters their PIN in a transaction process.

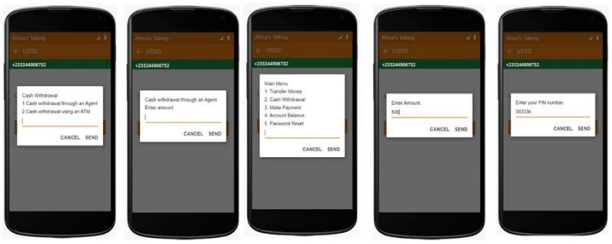

Figure 5: A summary of user PIN of six characters.

DISCUSSION

There are some participants who use "digit of their phone numbers" from the given phone number scenario (0244 906 732) for clarity. Some users used the last four (4) digits of their phone numbers (6732); others used the first four (4) digits (4906) apart from the phone code (024, 020, 054, 055, 027). Considering the perspective of gender, most females used their last digit as a PIN compared to males, and most males used the first four digits of their phone numbers as a PIN compared to females.

There was some diversity in the category for those who used "year of birth"; (1934). Some used their year of birth as the PIN code, and some also used the year of birth of their boyfriends, girlfriend, fiancées, parents and kids. The same consideration about gender and their choice of these patterns for PIN codes, most females prefers using their year of birth or that of their boyfriends compared to males.

The final category is those who used "other" forms of key combination as their PIN. The PINs used by this category is grouped into two, those just by instincts and others by familiarity with some numbers; this includes generic numbers such as (1234, 7777, and 4321). The comparison based on the gender on those grounds indicates more males prefer using this method of randomly combining numbers for PIN than females.

CONCLUSION

The above analysis clearly shows that, with this information at hand, anyone who has access to others' phones can break into their mobile money accounts without any trace.

The simulation determination of increasing the length of the key used as a PIN for mobile money was achieved. The need and

suggestion to increase the length of user PIN is to make the service more secure than what is currently used. According to Jean-Paul, the duration of time needed to reveal the keys used with the use of a computerized system in a brute force method is longer if the length of the key is longer. The current application key used by the telecoms is four digits; this therefore clearly indicates the vulnerability associated with its use and risk to access by fraudsters.

The outline of alphanumeric keys and the ability to increase the length of PIN in mobile money banking services will go a long way to reduce the rate of fraudulent activities on mobile money services.

REFERENCES

1. Abooleet S, Fang X. The Role of Transaction Cost in the Adoption of Mobile Payment. 2021.
2. Ahmad A, Li K, Feng C, Asim SM, Yousif A, Ge S. An empirical study of investigating mobile applications development challenges. IEEE Access. 2018;6:17711-17728.
3. Arun Prakash R, Jayasankar T, VinothKumar K. Biometric encoding and biometric authentication (BEBA) protocol for secure cloud in m-commerce environment. Appl Math Inf Sci. 2018;12(1): 255-263.
4. Beaunoyer E, Dupere S, Guitton MJ. COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies. Comput Hum Behav. 2020;111:106424.
5. Bhalla R, Jeyanthi N. M2U2: Multifactor Mobile Based Unique User Authentication Mechanism. Int J Intell Syst. 2018;455-464.
6. Boden J, Maier E, Wilken R. The effect of credit card versus mobile payment on convenience and consumers' willingness to pay. J Retail Consum Serv. 2020;52:101910.
7. Bryant J, Holloway K, Lough O, Willitts-King B. Bridging humanitarian digital divides during COVID-19. HPG (ODI).2020.
8. Chi T. Mobile commerce website success: Antecedents of consumer satisfaction and purchase intention. J Internet Commer. 2018;17(3): 189-215.
9. Corbitt BJ, Han YT. Trust and e-commerce: A study of consumer perceptions. Electron Commer Res Appl. 2003;2(3):203-215.
10. Dahlberg T, Mallat N. Mobile payment service development: Managerial implications of consumer value perception. Proceedings of the European Conference on Information Systems. 2002;649-657.
11. Feng W, Zhou J, Dan C, Peiyan Z, Li Z. Research on mobile commerce payment management based on the face biometric authentication. Int J Mob Comput Multimedia Commun. 2017;15(3):278-305.
12. Gao F, Rau PLP, Zhang Y. Perceived mobile information security and adoption of mobile payment services in China. In Mobile Commerce: Concepts, Methodologies, Tools, and Applications. 2018;1179-1198.
13. Ghannam R, Sharevski F, Chung A. User-targeted denial-of-service attacks in LTE mobile networks. In 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications. 2018;1-8.
14. Hillman S, Neustaedter C. Trust and mobile commerce in North America. Comput Hum Behav. 2017;70:10-21.
15. Hossain SA, Bao Y, Hasan N, Islam MF. Perception and prediction of intention to use online banking systems: An empirical study using extended TAM. Int J Acad Res Bus Soc Sci. 2021;9(1):112-116.
16. Iman N. Is mobile payment still relevant in the fintech era?. Electron Commer Res Appl. 2018;30:72-82.
17. Jibril AB, Kwarteng MA, Pilik M, Botha E, Osakwe CN. Towards understanding the initial adoption of online retail stores in a low internet penetration context: An exploratory work in Ghana. Sustainability. 2020;12(3):854.
18. Komulainen H, Saraniemi S. Customer centricity in mobile banking: a customer experience perspective. Int J Bank Mark. 2019;37(5):1082-1102.
19. Korableva ON, Durand T, Kalimullina OV, Stepanova I. Usability Testing of MOOC: Identifying User Interface Problems. In ICEIS. 2019;2:468-475.
20. Kwateng KO, Atiemo KAO, Appiah C. Acceptance and use of mobile banking: An application of UTAUT2.J Enterp Inf Manag. 2019;32(1):118-151.