International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, 2020
ISSN: 1475-7192

High Correctness Mobile Money Authentication System

Fouad Osman* and Hiroshi Nakanishi

Abstract--- *Mobile money is a mobile embedded system that is used for money deposit, money withdrawer, items purchase, bills payment, airtime and internet recharges. The current mobile money authentication system uses personal identification number (PIN) that is feeble, vulnerable to shoulder surfers and susceptible to mobile money attackers. To solve this flaws of mobile money authentication system and to establish high correctness mobile money authentication system. A new mobile money authentication system is studied. Key aspects for high correctness of mobile money authentication system is to correctly accept real mobile money users and to properly reject mobile money non-users. To correctly evaluate the mobile money users by the authentication system, mobile money system should have functions to identify and verify the users and functions to authorize the transactions of the money. To detect the mobile money user, a unique identity number is registered during mobile money user enrolment. To verify the identity of the user and authorize transactions, iris biometric authentication system is proposed and added in to the mobile money system. Iris biometric system is the most secured, robustness and reliable authentication system. It is real time verification system that cannot change with age and have minimum accuracy error rate. Users can easily accept Iris biometric system as mobile money authentication system because mobile camera can take the eye-iris images. In this paper a high correctness mobile money authentication system is propose that is based on iris biometric system and unique user ID number. The paper also outlines qualitative approach, interviewed number of mobile money users from their point of view and perspectives about the proposed iris system. Results show that most of the interviewee are highly welcome security strength to mobile money, particularly iris authentication system. Finally the paper discuss future research opportunities and limitations of the study.*

Keywords--- *Mobile Money, Personal Identification Number, Iris Biometric, Aliveness and Artifact Detection, Imposter.*

I. INTRODUCTION

Security and authentication consistencies are the foremost aspects for creating and preserving customer reliance, trust and expectations in mobile money services. Unfortunately mobile money service users rely on personal identification number (PIN) that is weak, vulnerable and can be easily guessed, misused and forged.

Mobile money technology provide three important basic service to its users which are mobile money transfer, mobile banking and mobile payments. By using mobile money service, the user can send and accept money to and from others (B.Mtaho, 2015). If the service provided by mobile money system providers to the users and customers is not guaranteed and assured to be secure and protected, then clienteles will be forced to have a second thought

Fouad Osman, Intellectual Property Ikohza (IP), Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Jalan Semarak, Kuala Lumpur, Malaysia. E-mail: mogue14@gmail.com*
Hiroshi Nakanishi, Intellectual Property Ikohza (IP), Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Jalan Semarak, Kuala Lumpur, Malaysia.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

which is leaving from the system and that is why security of mobile money service is paramount to the mobile network operators (Chong, 2006).

Vulnerability and the exposure of unstructured supplementary service data (USSD) mobile money security technology is based on the application of personal identification number (PIN). The security flaws of mobile money service is that the PIN number is transferred via USSD to the system server as a plain text, which gives an opportunity to the attacker who use network sniffers applications like wire-shark which can interfere and exploit mobile money systems (B.Mtaho, 2015). The noticeable information carried out by USSD is also visible to the service provider who can read the PIN and can manipulate customer's electronic currency (Chong, 2006). Furthermore malware attacker tries to find way to capture the codes of the USSD and apply the gained information to exploit android devices (Dobie, 2012)(Svajcer, 2014).

The present mobile money security identification and transaction authorization system that identifies the genuine users and authorize transaction is exclusively based on personal identification number (PIN) in which the subscriber use when performing transaction activities like bill payment, cash withdrawal, money transfer, air time and internet recharge. The problem with this authentication security features is that the personal identification number (PIN) is very short and consists of only four digits with no letters, symbols and combination of letters and numbers, which makes simple and easy for the shoulder surfers. Moreover, PIN is not masked and it is written in a plain text which increases the susceptibility and vulnerability to the snoop attacker (B.Mtaho, 2015). Another critical problem for the present mobile money authentication is that the same four digit numbers are used to authenticate users, identify subjects and authorize all the transaction activities that are taking place in mobile money services. These activities that are taking place within the mobile money are huge operations that are not limited to from transferring money to withdrawal, from paying bills to utility payment, from internet recharge to airtime recharge and from checking current balance to checking bank account balances through this mobile money system.

Furthermore, family members always share the PIN which also complicates the security vulnerability and risks of the system. Some research studies (Camner, Pulver, & Sjöblom, 2009) results have shown that the large number of mobile money service customers use date of birth (DOB) as their mobile money authentication PIN, which increase the percentage of guessing the users PIN. This kind of propensity directs to a critical security susceptibility as birth of date can be found in different sources like co-worker, family members, friends and countless management system logs (Camner et al., 2009). In addition to all that if user's mobile is lost or stolen there are no fortification techniques in which the impostor can be stopped from trying to figure out a way to crack down the PIN (Svajcer, 2014), apart from the user going to the mobile network operator (TNO) office and reporting the incident and disconnecting the SIM card operation from that stolen or lost mobile, which will take time the user to go there and will take process of disconnection. The rest of the paper work is organized as follows. Section 2 describes literature review of mobile money; section 2.1 is the history mobile money while Section 2.2describes the Current Mobile money authentication system. Section 2.3presentsIris Biometric which is the most secured biometric authentication system. Section2.4 describes Spoofing Attacks on Iris which is one of the weaknesses of biometrics and iris is no exceptional. Section 2.5 summarizes aliveness Detection which is a method used to prevent spoofing attacks on iris and other biometric systems while section 2.6points out Iris Cameras that is provided by smartphone mobiles.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

Section 3 is the methodology of the research study which is qualitative and design research. Section 4 is the results and findings of the study while section 4.1 explains the proposed and designed system of high correctness mobile money authentication system followed by section 4.2 which summarizes the limitations of the study and finally section 5 is the conclusion of the paper study.

II. LITERATURE REVIEW OF MOBILE MONEY

Cell phone devices are now the storage treasure for sensitive personal information which are not limited to bank details, password, PIN, confidential personal and business information. Smartphone mobiles are now the main infrastructure for online banking, online purchases, money transfers, bill payment and so on. In addition to that most of the smartphones that users carry in these days are so exclusive and expensive devices. According to those attributes cell phones have personal interest from the attacker (B.Mtaho, 2015). In 2009 computer crime and security survey stated that 42% of the participants of a survey conducted have experienced mobile device and laptop lost or burglary and another 12% experienced data breaches (Guo et al., 2004). Internet viruses can also hit cell phone devices, as NISA (Richardson & Director, 2008) described that because of the user's ignorance and inexperience, they install application from untrusted sources. In general cell phones have numerous security settings that by default are left-hand by manufacturer without being activated. If the consumer do not empower these kinds of feature it may lead to online interferences of the sensitive data like user's PIN to a possible third party (Hogben & Dekker, 2010).

Customer behavior, the cell phone and SIM card owner's behavior of the mobile money account has the sole responsibility of upholding and maintaining the security features of its mobile money account. The way that cell phone, SIM card and PIN are controlled my directly affect security of the automated money deposited in the account of mobile money. For instance some of the users share their PIN with the mobile money agents and family members when withdrawing money and transferring money respectively. This kind of activities may lead to security breach and illegal authorization accessibility of the mobile money account (B.Mtaho, 2015).

The working and the living atmosphere of the mobile money also affect the security risks of mobile money. Some of the mobile money agents carry out the operation of mobile money business, in which the mobile money agents have branches in villages and districts, but they also have external staff which are not mobile money network operator employee. These external staff they have their own business and they help the mobile money agent to help with money operations within their same shops. Some of dishonest staff may commit unauthorized transaction accessibility because they have the PIN of the mobile money service employee who works for the mobile money company. In addition to that some of the mobile money agent staff don't own an office, they do the operation by standing along the streets and road which make them more vulnerable and may lead to unauthorized access attack (B.Mtaho, 2015). Without robust authentication and authorization methods are applied, security of mobile money service will always remain at risk.

A. History of Mobile Money

Almost twenty years from today, the first mobile money transaction was conducted in 1997 in a mobile device. Coca Cola tested first SMS payment acceptance system from vending machines in Finland (Dahlberg, Guo, &

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

Ondrus, 2015). Mobil money serving as unbanked service provider became active in 2001. But it was in 2007 when mobile money gained the public attention and brought in to international prominence by the establishment of M-PESA Kenya (Aron, 2017).

After that mobile money service expanded its coverage all over the world. There are very little countries on earth that does not use any kind of mobile money today.Mobile money is transfer of physical cash in to an equivalent number of digital data (Vizzarri & Vatalaro, 2014) that can be transferred from mobile money account to another, can be purchased items, can be withdrawn from mobile money accounts electronic currency to hard cash, can be paid in utilities and so on. Some of the mobile financial services are bill payments, person to person mobile account transfers, proximity and remote payments of good and service, prepaid and airtime, internet charges and personal mobile accounts connection to bank accounts where customers can credit and debit their cash money. Everybody knows that money is extraordinarily attractive to fraudsters and cypher attackers (Gaber, Gharout, Achemlal, & Pasquet, 2012). As GSM mention in his 2016 report Mobile money is now almost in use in more than 93 countries all around the world (GSMA, 2017) with sub-Sahara Africa, South Asia and Latin America and the Caribbean are the leading continents.

B. Current Mobile money authentication system

There are three common basic access technology in mobile money, these are unstructured supplementary service data (USSD), subscriber identity module (SIM) toolkit-STK and short message service (SMS) (Guo et al., 2004). USSD which is a procedure for global system for mobile communications (GSM) provide supporting communication between cellphones and service provider computers or servers. USSD empower instantaneous and real-time session to be commenced between the cellphone user and the platform of the USSD application. When the service is invoked it documents data to be conducted and sent back and forth between the mobile user and the USSD application platform until the provision is finalized (Richardson & Director, 2008). When the session dismisses the USSD platform application, SMS which is configured in the system will be sent to the mobile money user through short message service center on the global system for mobile communication network. With the help of STK, the application on the SIM card permit users to access through their cellphone menu (B.Mtaho, 2015). As (Divya & Janani) stated, proximate opponents can perceive during the PIN entry, particularly mobiles which more efficiently in congested spaces than any other devices. Problem with the users of PIN is that they pick the same PIN for different resolutions and practice it so frequently. This may increase conceding the PIN which may put jeopardy on the user's money and data. The following figures illustrates the present mobile money authentication enrolment and execution phases(Mtaho, 2015).

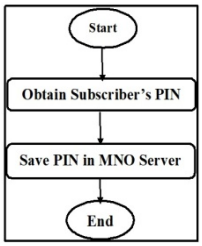

Figure 1: Mobile Money Authentication Enrolment Phase

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

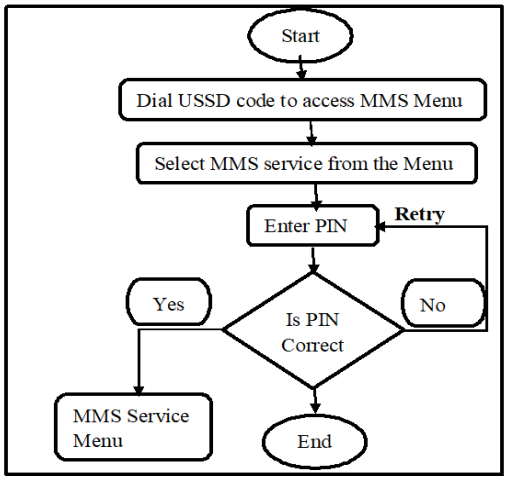

Figure 2: Mobile money authentication execution phase

As we see from these previous scholar studies PIN and password can no longer keep us safe, especially when technology advancement is faster than the rays of the sun and the intruders, imposters, easy money makers and attacker are sniffing around and developing sophisticated cracking software application. Therefore, the researcher propose a biometric mobile money authentication system that will enhance the correctness and the performance of mobile money authentication system. The rest of the literature review is based on the proposed biometric particularly iris authentication details and descriptions. It also explains the weaknesses of the iris like other biometrics and how to improve it, so that we get a high correctness mobile money user authentication system.

C. Iris Biometric

According to Priti and her colleagues (Miss. Priti V. Dable, 2016) stated that human being have biological traits of their own, a unique characteristics, an attributes that disparate one person from another during verification and identification of an individual for either allowing accessibility of a system or controlling the use of resource of an application. These unique human characters are known as detection of biometrics. Biometric physiognomies that even left and right eyes of the same person have different features.

The author defined iris as a small portion that is part of the sphere around the pupil of the eye. Though when associated to whole area of the human body iris has relatively contracted section, its prototype is very unique and dissimilar in each person and the sample will endure constant. Apart from being steady for decades, the texture of the iris is very exclusive that each person's minutiae are differing from the others. Eye surgery cannot modify the traits of the eye and can not cause any vision impairment.

Iris recognition systems have been applied by the researcher for the purpose of identification and authentication of the subjects, because iris technology is perfect for recognition rates and they are very reliable biometric traits. The most commonly used technology for iris recognition are communication network and mobile commerce authentication and transactions respectively, because iris are captured by using infrared and video cameras. Iris attributes are also very important for identifying subject from large database and have good accuracy and speed (Solanke & Deshmukh, 2016)

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

Iris patterns are unique from left to right and from subject to subject. Iris is very essential for system identification, authentication and verification because of the following reasons (Rajesh, Karnan, & Sivakumar, 2014)

I. Iris accuracy error rate is minimum
II. Iris does not change with age and it is a permanent biometric system
III. Users can easily accept because mobile camera can take the eye-iris image
IV. Iris is a real time verification system
V. Spoofing attacks resistance are very high in iris systems
VI. Some of the advantages of the iris for being a reliable biometric system for authorization are as follows (Miss. Priti V. Dable, 2016)
VII. Age does not change iris patterns
VIII. Iris is inside the eye in which it is protected and insulated from the environment around it
IX. Iris is simple and easy to implement through systems and application
X. The process of iris pattern matching speed is very fast

In our daily lives authentication and security are the two most important things. Iris biometric traits are one of the most trustworthy and reliable method a subject can be identified, authenticated or authorized (Tania, Motakabber, & Ibrahimy, 2014). Because they are inside the pupil of the eye and they are inside the eyelids and they are contactless with the iris sensor.

Iris recognition is considered the most accurate and reliable biometric traits due to texture uniqueness. Iris biometric modalities are secure, accurate and reliable because of its highly unique attribute structure of iris tissue (Kohli, Yadav, Vatsa, Singh, & Noore, 2016). Iris is applied and used in many application that are not limited to national ID projects, security border check and large scale identity applications.

For all above mentioned demonstrations of iris clarification, security strength, robustness and reliability, the researcher selected iris as a mobile money transaction verification and authorization. Iris is compatible with mobile cameras that is the most flexible to smartphones and they can be used to mobile money security features.

However, iris biometric features are susceptible to demonstration and presentation attacks. Presentation attacks are commonly known as spoofing attack which is an effort to conceal and mimic identity. These people who are trying to present spoofing attack on iris like they do on other biometric systems. These intruders want to access the iris protected system resources, locations and seepage system recognition by gaining unauthorized and illegally entry. During designing iris security system identifying and detecting spoofing attacks is a paramount to the system structure and is an ongoing academic topic (Kohli et al., 2016).

D. Spoofing Attacks on Iris

There are several types of spoofing attack on iris recognition system

Print/fake iris image: iris images can be printed in order to make a copy or scanned from the genuine user iris image. The coped iris image can then be used in a purpose of impersonating other subject identity (Kohli et al.,

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

2016). Gupta et al (2014) stated that scanned + printed or printed + captured image attacks can diminish the system accuracy verification to less than 10% at 0.001% FAR (Gupta, Behera, Vatsa, & Singh, 2014).

Iris image synthetic: spoofing attacks can create synthetic iris images that can boob and fool the system of the iris recognition. Iris features are embedded in to other subjects iris and assume that extraction mechanism of the iris know it (Venugopalan & Savvides, 2011). (Galbally, Ross, Gomez-Barrero, Fierrez, & Ortega-Garcia, 2013) suggested a method based about technique of iris image synthetic creation, the proposed method generate iris features similarity in which iris image synthesis matched with the genuine user iris code.

Contact lenses texture: texture contact lenses are cheap in price and are being used in both adjustments of the eyesight and cosmetic and beautifying purposes. They cover the original iris texture with lens thin texture that can affect the performance accuracy of the iris recognition system (Kohli et al., 2016)

Image acquisition

In reference to the work of (De Jesús, Máximo, Raúl, & Gabriel, 2016) on smartphone image acquisition, the capture of the image of the eye is very important for the recognition of the iris process. Acquiring high quality precision image depends on avoiding and removing the faultiness and limitations like light reflection, brightness of the environment, eyelashes and eyelids that cover the iris region.

E. Aliveness Detection

When biometric authentication selection is taking place an aliveness detection method is used by knowing how spoofing can be detected and rejected from the system. (Akhtar, Michelon, & Foresti, 2014) defined spoofing "spoofing occurs when an impostor attempts to masquerade as a genuine user by falsifying biometric data and thereby gaining illegitimate access" to the system). Weaknesses of biometric identification and verification to spoofing attacks are globally accepted facts (Akhtar et al., 2014). Aliveness detection methods decide or determine whether a subject contacting the biometric sensor technology is live subject or an artificial replica. By the use of aliveness detection methods for biometric trait spoofing, we can classify the weaknesses and vulnerability of each biometric trait.

In the proposed mobile money authentication system, an aliveness and artifact is added that will detect if the presented image is from a live person or an artifact. When the detector detects the sample image it will determine whether to accept the image for further processing or terminate the process operation.

F. Iris Cameras

The colored section of the eye is known as Iris and it occurs between the lens and cornea. It has the shape of a circle (spherical) with essential fleabag called the Pupil. The primary purpose of the iris is adjusting and monitoring the amount of light going in to the eye. There are muscles that are so tiny and let the required amount of light to enter the eye(Yanoff, 2014).

The detailed material of metabolic, hormonal, structural and biochemical operative of the human body are logged in numerous organization of the eye such as retina, staircase, cornea, iris pupil and conjunctiva which offers possibilities to sightsee and examine the data stored in the iris using processing images (De Jesus et al, 2016).

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

As detailed by (Shah & Shrinath, 2014) high standardized camera should be employed for the process of acquiring iris images for the application of natural light and infrared light. Location of the camera obtaining the image plays an important role whether it is used automatic or manual camera.

Application of mobile device camera for the capture of the iris image, the mobile camera has to deliver approximately resolution of around 70 pixels radio in the iris. Naturally the resolution of most cameras available in mobiles is in the rage of 100 to 140 pixels (De Jesús et al., 2016). This kind of resolution pixel or more than that would be enough to acquire iris image from mobile camera which proves that iris authentication system can be implemented and deployed in mobile money devices.

From left eye to the right eye iris has the characteristics of being unique even the identical twins have different iris patterns which remains unaffected and unchanged throughout subject's lifetime. According to the biology development study iris overall structure is naturally resolute the actual characteristics and aspects of its minutiae which are reliant on surrounding circumstances such as the iris embryonic predecessor situations(Chirchi & Kharadkar, 2011).

Mobile devices or smartphones have an embedded camera that are used for normal pictures and recording videos. This smartphone camera can process digital images which improve the image enrichment and can process image data accordingly. In addition to that the smartphones have the capacity to process the data that are conservative to process of the computer. According to (De Jesús et al., 2016) when processing the data of the digital image in a smartphone equivalent amount of resource capacity are needed. The resources are included but not limited to the mobile memory, storage space and processing time. The capacity that data processing take place have to be substantially abundant for the execution of the data being processed, otherwise it will affect the response speediness and the performance of the system.

III. METHODOLOGY/MATERIALS

Methodology is a framework or model that the researcher use with in the paradigm perspective. It is the researcher choice from one method over another (Wahyuni, 2012). The methodology approach of this paper is divided in to two phases. The first phase is based on qualitative research. A research method refers to the process or steps that are followed when conducting research study(Wahyuni, 2012). The research method is structured in to two sections, the nature of the knowledge with research reasons and methods carried out effective research(Walliman, 2017). The method of the qualitative approach of the paper study is based on case study that is non-probability sampling because it is pre-determined reasons.

Research techniques of this paper review is based on interview. Interview is chosen over other methods because in qualitative case study method, interview are more suitable for questions that needs probing to obtain an adequate information from the participants. The type of interview being selected is structured standardized ones (Walliman, 2017), (Kothari, 2004). The interview are very simple and short probing mobile money users' perspectives on current mobile money authentication system. The applicants being interviewed are 15 participants from mobile money users in two different countries, Kenya and Somalia.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

To answer the mobile money authentication vulnerability and the needs of the mobile money user the author found in the first phase of the study, we proposed a better mobile money authentication system that will enhance the mobile money user security.

The second phase of the methodologystudy of the paper is fundamentally based on design scienceresearch (Vaishnavi & Kuechler, 2004) where we constructed high accurate mobile money authentication design method. The system construction is based on design, concept or the architecture of the proposed high accurate mobile money authentication system. Because this is a science of the artifact (Vaishnavi & Kuechler, 2004)where the man-made objects and phenomena are constructed and designed to meet the required goals. The design of the high accurate mobile money authentication system design consists of mobile money user ID number, iris biometric traits, aliveness and artifact detection method and imposter removal method. This will provide users a high accurate, reliable and user trust mobile money system.

IV. Results And Findings

The following section explains the data analysis of the interview questions that have been collected from a selected mobile money customers and users. The participants of this case study are mobile money users or customers who live different countries that are common in mobile money usage. These countries are Kenya and Somalia, Kenya use a mobile money system known as M-PESA with more than twenty millions of users while Somalia use a mobile money system called ZAAD with millions of subscribers and users. The reason that those two countries where selected is that these countries are where mobile money system usage is very prominent and it is because the participants targeted are merchants, telecommunication network operator providers and mobile money users. The interview which is structured interview consists of four questions with question four consisting three sub questions. The details of the questions and their analysis are elaborated below.

By answering the questions of how users perceive the present mobile money authentication system. Some of the participants stated that mobile money authentication system is good, easy to use and makes life easy but it is weak and exposed, while others mentioned that the system's authentication method is not secure and is not satisfactory because of its vulnerability features. Most of the participants agree that improvement of the current mobile money authentication system is necessary and a paramount. Telecommunication network operators have to consider other options that are more secured mobile money authentication system than the current mobile money authentication system. These participants mentioned biometrics as better example of mobile money authentication system than PIN.

Responses referring to the questions of how much users think that PIN is secure stated that most of the participants think that PIN is not secure and it is weak that it is easy to gain access the system carrying the mobile money by simply guessing the PIN because the digits of PIN are very short and there are no combination of letters, numbers and symbols. Some others mentioned that the system is susceptible to intruders and PIN can be stolen or shared with other people that makes the mobile money PIN weaker.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

Interviewee answering the question of vulnerability of the current mobile money authentication system stated almost all of the participants interviewed in the study think that mobile money authentication system is vulnerable while very few of them think that the system is not vulnerable.

Answering the type of mobile money authentication security system users will prefer to use their mobile money system instead of PIN. Most of the participants would prefer a better mobile money authentication method than the current mobile money security system which is Pin. Some of them stating that biometrics like fingerprint, iris, and voice recognition and face recognition authentication methods are best authentication security methods for mobile money. Very few of them proposed password, multi-factor authentication methods with security questions that may make the system more secure and users trust more and could be reliable choices.

4.1 High correctness mobile money authentication system design

The high correctness mobile money authentication system is based on the ideology of unique user ID number and biometric traits particularly iris that is the most secured, robustness, reliable and the most compatible on smartphone mobiles. The new mobile money authentication system, mobile money users first provide their unique ID number that were given during enrolment. The entered user ID is identified whether it belongs to the user and is registered on the database. When identified the user ID number process is proceeded in to the next level. If identification fails process is terminated. After user ID identification, mobile money user provides his/her iris traits by scanning the iris features by using smartphones near infrared (NIR) camera.

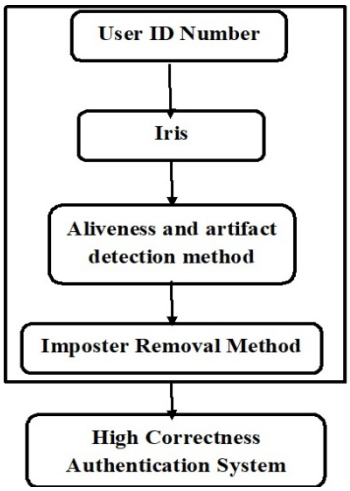

Figure 3: high correctness mobile money authentication system

After processing the captured iris image, an aliveness and artifact detection method determines whether the processed iris images are from live subject or from artifacts. Aliveness and artifact detection method is a method that detects whether the image presented to mobile money authentication system belongs to a living mobile money user or is an artificial images that are used as a spoofing attacks. Spoofing attacks are synthetically produced artifacts. Iris artifact can be well-made eye model, synthetic iris, contact lens, video iris and printed iris. When aliveness and artifact detection method determines that iris images are from live subject, the images are proceeded to the next level, if images are determined as an artifact the process is terminated.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

After the detection of subject aliveness, an imposter removal method checks whether the processed images are from real mobile money user owner that is referred to as genuine user or from individual that is not registered in mobile money system that are referred to as imposters. Imposters are subjects that are falsely identified as valid user though they are not enrolled in mobile money system. Imposters are real/live subjects (not artifacts) that are not registered in the system and the system wrongly grant access as a legitimate user. Genuine user is a person that is registered in to the mobile money system and his/her data is stored in the mobile money database. In here genuine users can be identified by using their unique ID number and their iris traits. Unique ID number and iris images are fused during user enrollment and they can be matched as a batch during identification and verification.

Imposter removal method ensures the compatibility and similarity of the user ID number and the processed iris images. If they match, then mobile money system accessibility is granted if not then it is blacklisted as an imposter. After access is granted mobile money users can navigate through the mobile money system by sending money, withdrawing money, paying bills and so on. This high correctness mobile money authentication system can enhance the security features of the mobile money. it can also provide mobile money users reliability and trust the mobile money system.

4.2 Limitations

Limitations of this study is that smartphones haven't yet implemented the iris camera in to the mobile camera. There are ongoing endeavors (Ali, Shah, Javed, Abdullah, & Zafar, 2017) and this new authentication technology will be soon available in the smartphone cameras. The other limitation of the study is that there are no simulation experiments that the researcher has carried out in order to evaluate the practicality of the new proposed high correctness mobile money authentication system. Researchers can carry out further study on either simulation experiments or practical mobile money application for the proposed mobile money authentication system.

V. CONCLUSION

In this paper we discussed the weaknesses and vulnerability of the current mobile money authentication system which is based on personal identification number (PIN). We also collected a quantitative data interviewing mobile money users how they perceive the mobile money personal identification number security vulnerability, weaknesses and their preferable mobile money authentication system. Most of the participants stated that the current mobile money security system does not have enough security features and they recommends biometrics authentication system as a better authentication system if upgraded to the current mobile money system. Therefore according the needs of the mobile money users we proposed high correctness mobile money authentication method consisting of personal unique ID number and iris with aliveness and artifact detection method and imposter removal method that will improve the user authentication features of the mobile money and will provide mobile money users confidentiality and reliability to the mobile money system. Further study can be carried out by other researchers on evaluating the proposed mobile money authentication system by using simulation experiments or by applying directly to any mobile money system.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

REFERENCES

[1] Akhtar, Z., Michelon, C., & Foresti, G. L. (2014). Liveness detection for biometric authentication in mobile applications. *Paper presented at the Security Technology (ICCST), 2014 International Carnahan Conference on.*

[2] Ali, S. A., Shah, M. A., Javed, T. A., Abdullah, S. M., & Zafar, M. (2017). Iris recognition system in smartphones using light version (LV) recognition algorithm. *Paper presented at the Automation and Computing (ICAC), 2017 23rd International Conference on.*

[3] Aron, J. (2017). 'Leapfrogging': a Survey of the Nature and Economic Implications of Mobile Money: Centre for the Study of African Economies, University of Oxford.

[4] B.Mtaho, A. (2015). Improving Mobile Money Security with Two-Factor Authentication (Vol. 109).

[5] Camner, G., Pulver, C., & Sjöblom, E. (2009). What makes a successful mobile money implementation? Learnings from M-PESA in Kenya and Tanzania. London: GMSA, available at: www. gsmworld. com/our-work/mobile_planet/mobile_money_for_the_unbanked/, accessed, 24, 2011.

[6] Chirchi, E. R. M., & Kharadkar, R. (2011). Improvement of Performance Evaluation for Iris Pattern Recognition. *International Journal of Computer Applications*, 34(6).

[7] Chong, M. K. (2006). Security of Mobile Banking:Secure SMS Banking.

[8] Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, 14(5), 265-284.

[9] De Jesús, R.-B. J., Máximo, L.-S., Raúl, P.-E., & Gabriel, G.-S. (2016). Methodology for Iris Scanning through Smartphones. *Paper presented at the Computational Science and Computational Intelligence (CSCI), 2016 International Conference on.*

[10] Divya, M., & Janani, A. Defending Shoulder Surfing Attacks in Secure Transactions Using Session Key Method. *International Journal of Innovative Research in Science, Engineering and Technology*, 4.

[11] Dobie, A. (2012). How to Tell If Your Samsung Phone is Vulnerable to Today's USSD Hack.

[12] Gaber, C., Gharout, S. ı., Achemlal, M., & Pasquet, a. M. (2012). Security challenges of mobile money transfer services.

[13] Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., & Ortega-Garcia, J. (2013). Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Computer Vision and Image Understanding*, 117(10), 1512-1525.

[14] GSMA. (2017). State of the Industry Report on Mobile Money. from GSMA

[15] Guo, C., Wang, H. J., & Zhu, W. (2004). Smart-phone attacks and defenses. *Paper presented at the hotnets III.*

[16] Gupta, P., Behera, S., Vatsa, M., & Singh, R. (2014). On iris spoofing using print attack. Paper presented at the Pattern Recognition (ICPR), 2014 *22nd International Conference on.*

[17] Hogben, G., & Dekker, M. (2010). Smartphones: Information security risks, opportunities and recommendations for users. *European Network and Information Security Agency*, 710(01).

[18] Kohli, N., Yadav, D., Vatsa, M., Singh, R., & Noore, A. (2016). Detecting medley of iris spoofing attacks using DESIST. *Paper presented at the Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on.*

[19] Kothari, C. R. (2004). Research methodology: Methods and techniques: New Age International.

[20] Miss. Priti V. Dable, P. P. R. L. a. M. S. S. K. (2016). Improving Iris Recognition Performance using Acquisition, Segmentation and filter. *Paper presented at the International Journal on Recent and Innovation Trends in Computing and Communication*

[21] Mtaho, A. B. (2015). Improving Mobile Money Security with Two-Factor Authentication. *International Journal of Computer Applications*, 109(7).

[22] Rajesh, T., Karnan, M., & Sivakumar, R. (2014). Performance Analysis of Iris Recognition System-A Review. *International Journal of Computer Science & Information Technology*, 39-50.

[23] Richardson, R., & Director, C. (2008). CSI computer crime and security survey. *Computer Security Institute*, 1, 1-30.

[24] Shah, N., & Shrinath, P. (2014). Iris Recognition System–A Review. *International Journal of Computer and Information Technology*, 3(02).

[25] Solanke, S. B., & Deshmukh, R. R. (2016). "Biometrics—Iris recognition system" A study of promising approaches for secured authentication. *Paper presented at the Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on.*

[26] Svajcer, V. (2014). Not Just for PCs Anymore: The Rise of Mobile Malware.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020

[27] Tania, U. T., Motakabber, S. M., & Ibrahimy, M. I. (2014). Template Matching Techniques for Iris Recognition System. *Paper presented at the Computer and Communication Engineering (ICCCE), 2014 International Conference on.*

[28] Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems.

[29] Venugopalan, S., & Savvides, M. (2011). How to generate spoofed irises from an iris code template. *IEEE Transactions on Information Forensics and Security,* 6(2), 385-395.

[30] Vizzarri, A., & Vatalaro, F. (2014). m-Payment systems: Technologies and business models. *Paper presented at the Euro Med Telco Conference (EMTC),* 2014.

[31] Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies.

[32] Walliman, N. (2017). Research methods: The basics: Routledge.

[33] Yanoff, M. (2014). Ophthalmic Diagnosis & Treatment: JP Medical Ltd.

DOI: 10.37200/IJPR/V24I4/PR201466
Received: 16 Jan 2020 | Revised: 17 Feb 2020 | Accepted: 26 Feb 2020