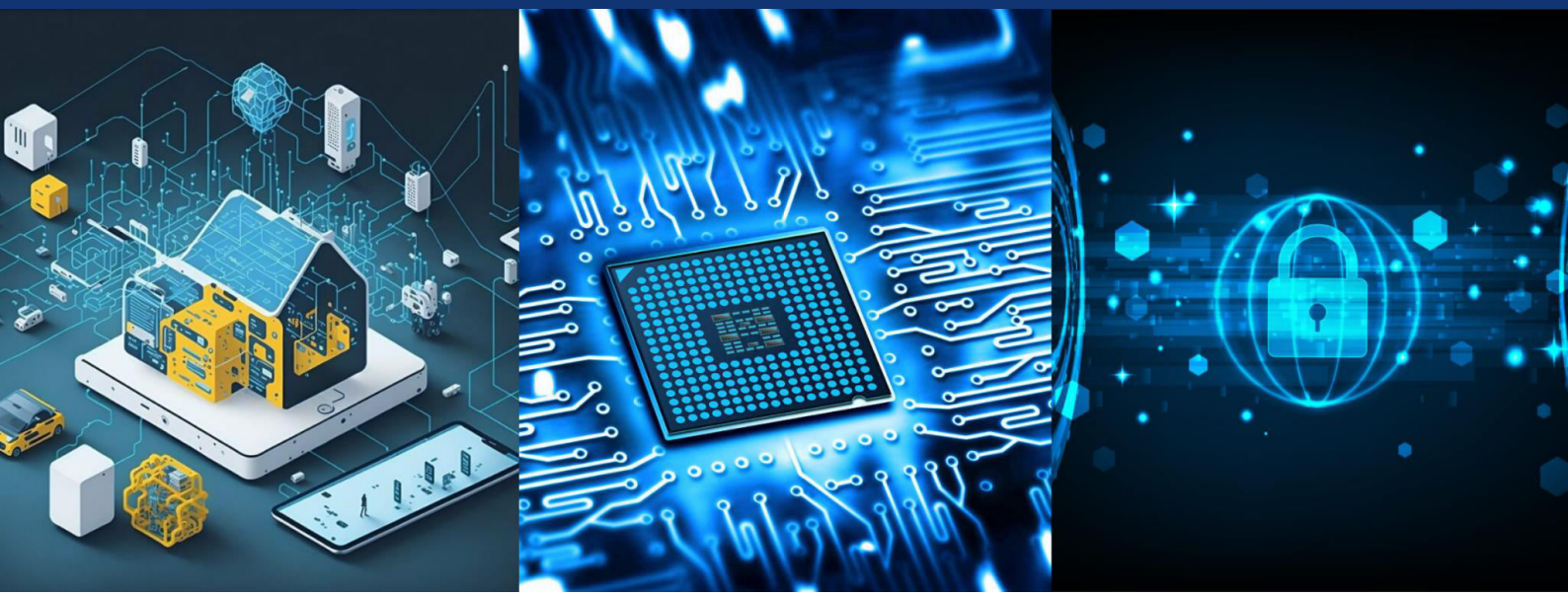
IJIRCCE

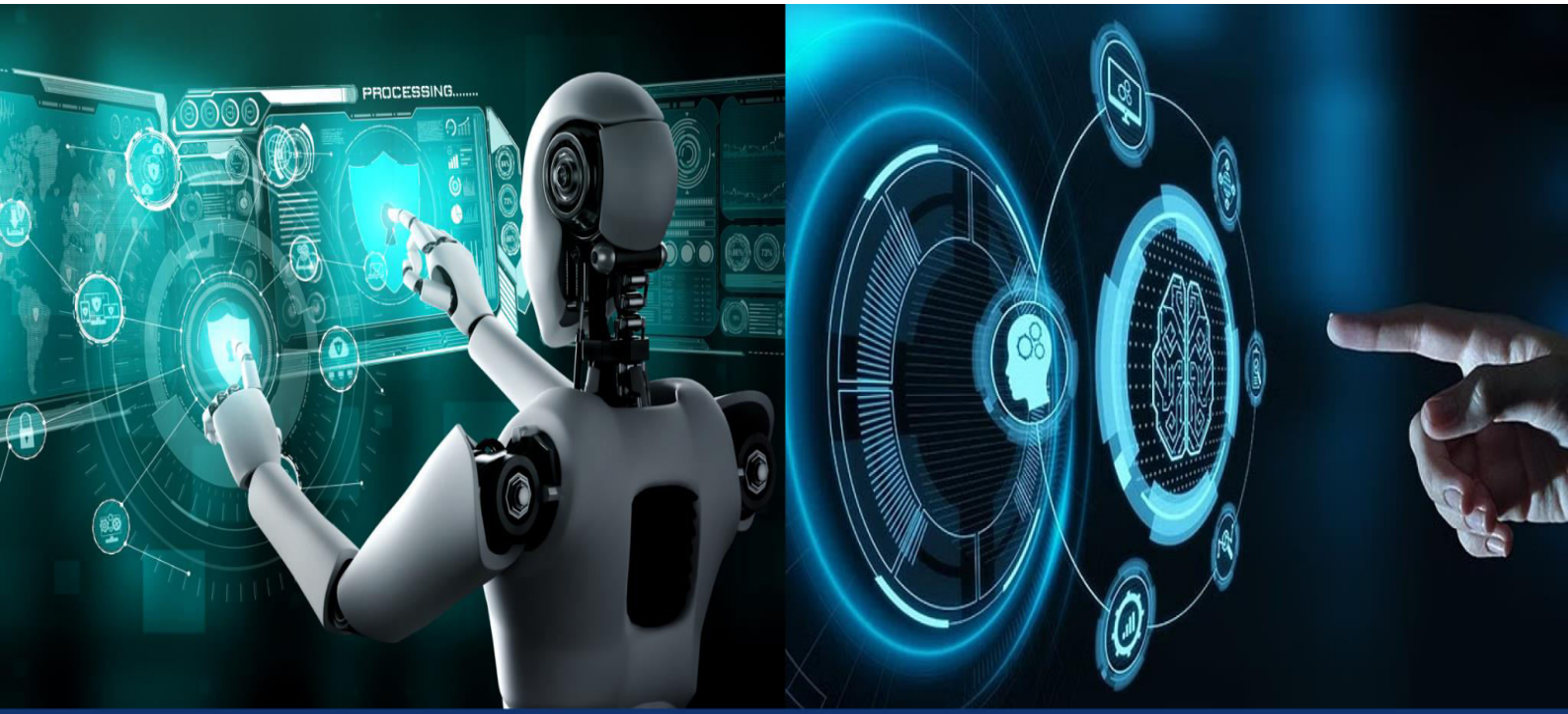
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 4, April 2025

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304198

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

An Two-Factor Authentication Scheme for Mitigating Risks in Mobile Payments

Mrs A Loganayaki

Assistant Professor, Department of Computer Science Engineering, The Kavery Engineering College, Mecheri, Salem, Tamil Nadu, India

Sree Prasanna I S, Dinesh K, Prakash A, Sanjay M

Department of Information Technology, The Kavery Engineering College, Mecheri, Salem, Tamil Nadu, India

ABSTRACT: The rapid adoption of mobile payment applications has transformed the way people conduct financial transactions. While these applications offer convenience and speed, they are also vulnerable to cyber threats, including unauthorized access and phishing attacks. Descriptive research papers and studies related to the theme were selected. Three reviewers extracted information independently on authentication, mobile money system architecture, mobile money access, the authentication scheme for mobile money, various attacks on the mobile money system (MMS), threat models in the 2FA scheme for mobile money, and countermeasures. Through literature analysis, it was found that the threat models in the 2FA scheme for mobile money were categorised into five, namely, attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity, and attacks against availability. The countermeasures include use of cryptographic functions (e.g., asymmetric encryption function, symmetric encryption function, and hash function) and personal identification (e.g., number-based and biometric-based countermeasures). This review study reveals that the current 2FA scheme for mobile money has security gaps that need to be addressed since it only uses a personal identification number (PIN) and a subscriber identity module (SIM) to authenticate users, which are susceptible to attacks. This work, therefore, will help mobile money service providers (MMSPs), decision-makers, and governments that wish to improve their current 2FA scheme for mobile money.

KEYWORDS: two-factor; authentication scheme; authentication; mobile money; the mobile money system; mobile banking; threat models.

I. INTRODUCTION

The rapid adoption of mobile payment applications has transformed the way people conduct financial transactions. While these applications offer convenience and speed, they are also vulnerable to cyber threats, including unauthorized access and phishing attacks. Traditional money transfer apps primarily rely on PIN-based authentication, which may not be sufficient to counter modern security risks. To address these challenges, this project introduces an advanced secure money transfer application that incorporates an OTP verification system before every transaction and location-based restrictions to ensure payments are made only in permitted locations. By leveraging Android Studio for application development and Python for backend processing, the system ensures a seamless and secure transaction experience.

The development By offering more than just electronic payment options, such as payment cards, digital and mobile wallets, electronic currency, contactless payment methods, etc., the development of the Internet and the emergence of e-commerce have facilitated the digitization of the payment process. Payment services are currently in a transitional phase as they gain popularity and move towards the rosy interim possibility of the future thanks to technological innovation. It's crucial to utilise a secure mobile payment solution to avoid this. The evaluation of the security of mobile payment solutions is the main objective of this study. The issue that users of this mobile payment system are running into has been identified in this work.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304198

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

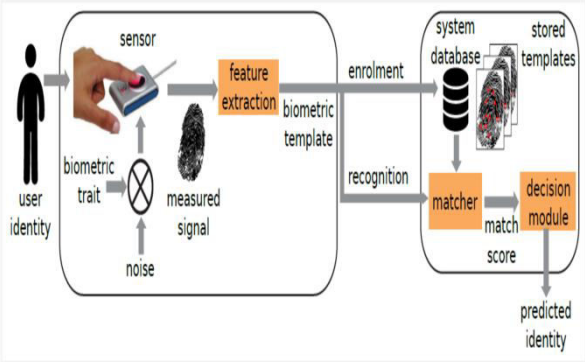


Fig 1: Secure and Efficient Multi-Factor Authentication

The risks related to these user questions are then determined by analysing them in accordance with the RBI guidelines and BASEL specifications. The study offers helpful data to evaluate the safety of your mobile payment solution and establish its level of risk in comparison to other options. Based on the findings of this study, generalisations can be made about the security of mobile payment systems in India. Users of mobile devices have increased thanks to the advancement of wireless technology, which has also sped up the development of electronic devices. Mobile transactions are commerce. These services enable users to conduct financial transactions using mobile money, dispensing with banks, ATMs, and credit cards in favour of mobile devices acting as business tools. After making an attempt to buy products or services from a business or service provider, a mobile user contacts a reputable third-party wireless service provider or financial institution to verify their identity and the value of the purchase. After passing the test, you can finish the transaction by using your mobile wallet. Users have the option of withdrawing money from their bank accounts, mobile wallets, or phone bills. In addition, a user has the option of paying with mobile money provided by another user or a different mobile service provider.

II. LITERATURE REVIEW

Customers' understanding of the security of mobile payment options is crucial to the market acceptance of related systems. We examine security concerns with mobile payments from the viewpoint of the customer in this article. We analyse empirical data from the MP2 Mobile Payments Survey, which included 8295 respondents, based on theoretical studies in order to develop a set of dimensions, categories, and dimensions. The findings have both scientific and useful implications. They serve as the foundation for choosing the right metrics for additional empirical research. A guide for mobile payment service providers that explains how to design and communicate their payment processes effectively can also be helpful in convincing customers that their processes are secure by addressing their concerns in educational advertising.

According to-[Linck, Kathrin, Key Poust chi, and Dietmar Georg Wiedemann. "Security issues in mobile payment from the customer viewpoint." (2006): 1-11.] 2. Mobile payments at POS, mobile payments as POS, mobile payment platforms, independent mobile payment systems, and direct billing by mobile operators are the five categories into which mobile payment systems can be divided. Due to their convenience, mobile payments have gained popularity across many regions, but they are also vulnerable to numerous threats and security issues. This white paper describes each type of mobile payment system as well as the model for processing mobile payments. List the security services needed for mobile payment systems as well as the current security measures. We also list and describe three additional security risks. H. System vulnerabilities, data breaches due to SSL/TLS flaws, four security challenges, and malware.

According to -Wang, Yong, Christen Hahn, and Kruttika Starve. "Mobile payment security, threats, and challenges." 2016 second international conference on mobile and secure services (Mabises're). IEEE, 2016. 3. The purpose of this article is to evaluate the development of mobile payment research over the previous eight years. According to a previous review of the literature (Dahlberg et al. 2008b), the majority of studies between the years of 1999 and 2006 concentrated on just a few topics. A research strategy was created to address this problem and encourage researchers to

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

investigate novel subjects. Our research reveals that despite a limited amount of new knowledge and similar insights, researchers have continued to focus on the same issues (particularly consumer acceptance and technology aspects). I was. In addition to reviewing the literature, we also speculate on potential causes for the dearth of diversity in research and offer fresh suggestions for enhancing future studies on mobile payments. According to -[Dahlberg, Tomi, Jie Guo, and Jan Ondrus. "A critical review of mobile payment research." Electronic commerce research and applications 14.5 (2015): 265-284.]

4. New technological developments have sped up the development and rollout of numerous secure applications for smartphones. Mobile and computer devices allow users to access and manage their data in a flexible and secure manner, but when users share a lot of private information and confidential data through open devices and networks This adds a fresh level of security difficulties. Because of this, mobile operating systems are becoming more and more vulnerable to malware, which then compromises these applications and steals sensitive data. This document offers his Trust PAY mobile payment framework, which can guarantee the security of overpayment transactions and enable payments that respect users' privacy. It is built on the security-enhanced Truston platform. ARM FastModel and the Open Virtualization Software Stack for ARM Trust Zone were used to implement a prototype system in a simulation environment.

According to - [Kashiwa, Saleem, and Anwar Usman Shaheed Zulfiqar. "Analysis of mobile payment security measures and different standards." Computer Fraud & Security 2007.6 (2007): 12-16.] 5. Mobile payments present businesses with unrivalled new opportunities, but they also present new difficulties. One of the most important and challenging issues for mobile payments is mobile security. As more people use Internet-enabled devices, it is becoming a hot topic. Even though there are many wireless devices in use today, there is little security on mobile devices. As long as players only concentrate on launching mobile payment infrastructure, consumer adoption of mobile payment services will undoubtedly slow. In order to determine the advantages and disadvantages of the current mobile payment services, this study will examine mobile payments and security. Since there are many parties involved in mobile payment services, including operators, banks, and network (terminal) providers, it is also important to consider how these parties can grow their businesses.

Mobile payments, as defined by the Mobile Payment Forum, are financial transactions completed over mobile telecommunications networks using a variety of mobile user devices, including mobile phones, smart phones, PDAs, and mobile terminals. Mobile payments are financial transactions made using a mobile device for the purpose of confirming and making payments for goods and services. Payers may interact with merchants in person or remotely. Customers can use mobile payment systems to buy and pay for goods and services using their smartphones. Here, personal mobile devices are used for payment in connection with distance selling. Remote payments can be made from a bank or the recipient. An introduction to mobile payments is provided in this chapter.

The development of various forms of mobile computing technologies has exploded over the past two decades, allowing users to access services from a wide range of portable devices at any time and from any location. Mobile payment (m-payment) systems and applications are being developed and deployed more quickly thanks to technological advancements like low-cost, high-performance user devices (like phones), highspeed cellular access, secure communication protocols, and the Internet. It has spread quickly throughout much of the world. All parties interacting with the m-payments system must prioritise security (users, merchants, banks, etc.). The authors go over a number of security issues that should be taken into account when developing and putting into use a payment system. As part of supporting secure end-to-end m-Payment transactions, we also examine the security of his solution.

III. RESEARCH METHODOLOGY

The research design used in the study is descriptive. It is concerned with describing the security features as well as how mobile payment services are used. The study focuses on Indian mobile payment services. It is designed to assess security, define usage, and classify different mobile payment services. The secondary data is gathered from a variety of publications, websites, and articles. in order to determine the connection between the use of mobile payment services. In order to evaluate the security of the mobile payments services, a conceptual model is prepared with the aid of secondary data mentioned in the literature review. Secondary data sources are used to help categorise the mobile payments services.

© 2025 IJIRCCE | Volume 13, Issue 4, April 2025| DOI: 10.15680/IJIRCCE.2025.1304198

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

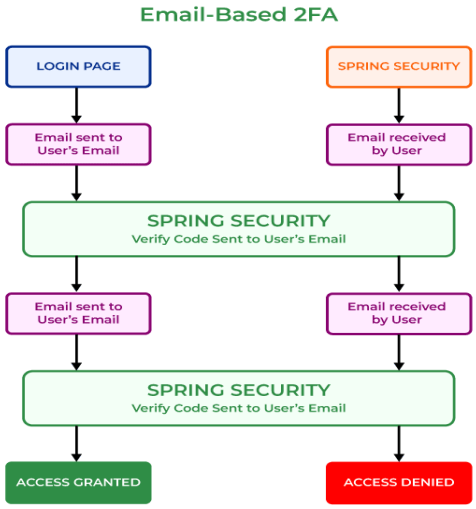


Fig 2: Spring Security – Two Factor Authentication

A conceptual model is created using secondary data from the literature review in order to assess the security of mobile payment services. The security of mobile payment services is then assessed using this model. The variables (in this model) used to measure the security of mobile payment services are determined using secondary data. Therefore, the conceptual model is built using secondary data. The study employed a mixed-methods research design that included the collection and analysis of both quantitative and qualitative data. An online survey and in-depth interviews with Indian users of mobile payments served as the study's main data sources. An online questionnaire was used to conduct the survey, and a sample of people who use mobile payments received it. The survey gathered information on how frequently mobile payment services are used, how secure they are, what users' top security concerns are, and how they feel about the security of these services.

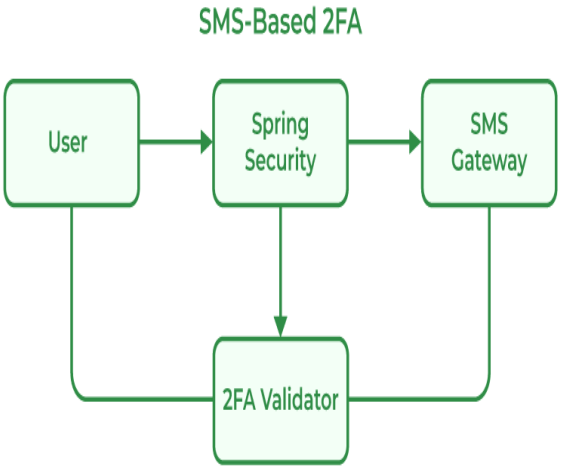


Fig 3: Two Factor Authentication | GeeksforGeeks

The Reserve Bank of India (RBI) and the Indian Banks Association (IBA) launched the National Payments Corporation of India (NPCI) as a project for the Retail Payment and Settlement System. The Payments and Settlement Systems Act of 2007 allowed for the establishment of the he organisation in 2008. The Reserve Bank of India (RBI), the Association of Indian Banks (IBA), and the National Payments Corporation of India (NPCI) different systems are unified into a unified and standardised business process at NPCI, which is registered under Section 8 of the Companies Act No. of

2013 as a "not for profit" company. It is made to connect to systems for retail payments or something comparable. The NPCI also wants to help the general public become financially included by promoting accessible payment technology. Operation of the National Payments Corporation of India's Check Cutting System, National Automated Clearing House (ACH), and Aadhaar Supported Payment System

IV. RESULT ANALYSIS

A crucial component of Internet security is the Public Key Infrastructure used in UPI payments. The cryptographic framework is made up of a number of technologies and procedures that secure and authenticate digital communications. A digital certificate that authenticates the device or user sending the digital communication is bound to a cryptographic public key by the PKI. Digital certificates serve as a kind of digital passport to confirm that senders are who they say they are and are issued by a reputable source, a certificate authority (CA). (hosted on your web server), as well as your client (a user attempting to connect via a browser). Additionally, it can be used to ensure that messages are only visible to the sender within an organisation through secure communications.

For users with entry-level phones or smartphones with spotty internet connectivity, UPI Lite is intended to offer a more straightforward user experience and facilitate basic payment transactions. The following are some advantages of UPI Lite in India: Increased Accessibility: UPI Lite was created to increase accessibility for users with entry-level smartphones or phones with spotty internet connectivity. This makes it simpler for more people to take part in the ecosystem of digital payments. User Interface Simplified: UPI Lite has a user interface that is simple to use and navigate. Users don't need to navigate challenging menus and options in order to complete simple payment transactions. Faster Transactions: UPI Lite provides a faster payment experience than traditional payment methods. transactions are completed in real time, eliminating the need for payments, reducing the time and effort required for payment transactions.

Fig 4: Multi-factor Authentication Market Size

A one-time password or a biometric authentication code could be sent to the user's phone as part of this. Antivirus Software: Users must install antivirus software on their mobile devices to guard against malware viruses. Malware that can be used to steal personal information is found and removed by antivirus software. Regular Security Updates: To

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

ensure that mobile payment apps have the most recent security features and safeguards, they should be updated frequently.

V. CONCLUSIONS AND FUTURE WORK

The advent of mobile money has enhanced the standard of living of the unbanked population in developing countries. As much as it offers a wide range of services and benefits, mobile money has experienced increases in attacks against the current 2FA scheme. This study conducted a review of the threat models and countermeasures in the 2FA scheme for mobile money. The authors utilised an appropriate search strategy to review the relevant literature.

With the comprehensive research and literature analysis, the threat models in the 2FA scheme for mobile money were classified into five categories: (1) attacks against privacy; (2) attacks against authentication, such as impersonation attack, replay attacks, masquerade attack, spoofing attacks, social engineering attack, phishing attack, and Trojan horse attacks; (3) attacks against confidentiality, such as eavesdropping attacks, brute force attacks, guessing attacks, and shoulder surfing attack; (4) attacks against integrity, such as MITM attack, salami attack, and insider attacks; (5) attacks against availability such as DoS and DDoS attacks, and mobile phone theft.

REFERENCES

1. Suri, T. Mobile Money. *Annu. Rev. Econ.* **2017**, *9*, 497–520. [**Google Scholar**] [**CrossRef**]
2. Grundmann, A.S. Feasibility Study of a Mobile Payment System on Kasadaka: A Sustainable Voice Service Platform. Bachelor's Thesis, Vrije Universiteit, Amsterdam, The Netherlands, 2018. [**Google Scholar**]
3. Kanobe, F.; Alexander, M.P.; Bwalya, K.J. Information Security Management Scaffold for Mobile Money Systems in Uganda. In Proceedings of the 18th European Conference on Cyber Warfare & Security, University of Coimbra, Coimbra, Portugal, 4–5 July 2019; pp. 239–248. [**Google Scholar**]
4. Uganda Communications Commission (UCC). *Telecommunications, Broadcasting and Postal Markets Industry Report Q2 (April–June) 2019*; UCC: Kampala, Uganda, 2019. Available online: **https://www.ucc.co.ug/wp-content/uploads/2017/09/Industry-Report-Q2-April-June-2019-Final.pdf** (accessed on 18 June 2020).
5. Bank of Uganda (BoU). *Bank of Uganda (BoU) Annual Report-2018/19*; Bank of Uganda: Kampala, Uganda, 2019. Available online: **https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/publications/Annual_Reports/All/Annual-Report-2019.pdf** (accessed on 14 July 2020).
6. Okeleke, K. *Uganda: Driving Inclusive Socio-Economic Progress through Mobile-Enabled Digital Transformation*; GSM Association: London, UK, 2019; Available online: **https://www.gsma.com** (accessed on 20 May 2020).
7. Darvish, H.; Husain, M. Security Analysis of Mobile Money Applications on Android. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 3072–3078. [**Google Scholar**]
8. Ali, G.; Dida, M.A.; Sam, A.E. Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda. *Information* **2020**, *11*, 309. [**Google Scholar**] [**CrossRef**]
9. Gwahula, R. Risks and Barriers Associated with Mobile Money Transactions in Tanzania. *Bus. Manag. Strat.* **2016**, *7*, 121–139. [**Google Scholar**]
10. Musuva-Kigen, P.; Ekpeke, M.; Inkoom, E.; Inkoom, B.; Masesa, D.; Kaimba, B.; Mbae, K. *Kenya Cyber Security Report 2016*; Serianu Ltd.: Nairobi, Kenya, 2016. [**Google Scholar**]
11. Castle, S.; Pervaiz, F.; Weld, G.; Roesner, F.; Anderson, R. Let's talk money: Evaluating the security challenges of mobile money in the developing world. In Proceedings of the 7th Annual Symposium on Computing for Development (ACM DEV'16), New York, NY, USA, 18–20 November 2016; pp. 1–10. [**Google Scholar**]
12. Buku, M.; Mazer, R. Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System. 2017. Available online: **http://www.cgap.org/publications/fraud-mobile-financial-services** (accessed on 11 March 2020).
13. Lonie, S. Fraud Risk Management for Mobile Money: An Overview. 2017. Available online: **https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf** (accessed on 12 February 2020).

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

14. Bosamia, M.P. Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. In Proceedings of the 2017 International Conference on Soft Computing and Its Engineering Applications (icSoftComp-2017), Changa, India, 1–2 December 2017; pp. 1–7. [**Google Scholar**]
15. Maseno, E.M.; Ogao, P.; Matende, S. Vishing Attacks on Mobile Platform in Nairobi County Kenya. *Int. J. Adv. Res. Comput. Sci. Technol. IJARCST* **2017**, *5*, 73–77. [**Google Scholar**]
16. Akomea-Frimpong, I.; Andoh, C.; Akomea-Frimpong, A.; Dwomoh-Okudzeto, Y. Control of Fraud on Mobile money services in Ghana: An exploratory study. *J. Money Laund. Control* **2019**, *22*, 300–317. [**Google Scholar**] [**CrossRef**]
17. Balasubramanian, S. Study of Cybercrime in the Banking and Financial Sectors. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2018**, *3*, 1205–1212. [**Google Scholar**]
18. Alhassan, N.S.; Yusuf, M.O.; Karmanje, A.R.; Alam, M. Salami Attacks and their Mitigation—An Overview. In Proceedings of the 5th International Conference on Computing for Sustainable Global Development, New Delhi, India, 14–16 March 2018; pp. 4639–4642. [**Google Scholar**]
19. Kunda, D.; Chishimba, M. A Survey of Android Mobile Phone Authentication Schemes. *Mob. Netw. Appl.* **2018**, *73*, 1–9. [**Google Scholar**] [**CrossRef**]
20. Phipps, R.; Mare, S.; Ney, P.; Webster, J.; Heimerl, K. ThinSIM-Based Attacks on Mobile Money Systems. In Proceedings of the COMPASS '18: ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS), New York, NY, USA, 20–22 June 2018; pp. 1–11. [**Google Scholar**]

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details