ISSN No:-2456-2165

Evaluation of Identity Access Management Frameworks on the Safety of Mobile Money Transactions used by FinTech Companies in Nairobi

Dennis Mwangi, Dr. Bonface Ratemo, Dr. Geoge Musumba

Abstract:- Smartphone technology improved access to mobile money which enabled FinTech companies successfully deploy service systems bringing massive benefits to those with limited access to banking. Embracing its usage has many security issues and challenges and the need to evaluate identity access management and maintenance associated with the safety of mobile money transactions. A descriptive research design was used with the target population in Fintech companies. Data collection techniques used were primary data through questionnaires while secondary sources of data were document reviews, official documents, publications, journals, reports, and online repositories. SPSS software was used on both qualitative and quantitative data to grasp the intent and rate at which physical access to IT assets, remote access management, users and devices authentication, access permissions; how authorization and network security are managed. Statistical techniques such as percentages, correlation and regression analyses were used. Findings revealed that key security issues were identity theft, authentication attack, phishing attack, vishing attack, SMiShingattacks, personal identification number (PIN) sharing, and agent-driven fraud. The use of better access controls, customer awareness campaigns, agent training on acceptable practices, strict measures against fraudsters, and high-value mobile money transaction monitoring, were some recommendations given. This study helps mobile money operators, mobile money decision makers, and the government to identify and evaluate key security issues associated with the safety of mobile money transactions in Fintech companies and recommendations proposed to address security gaps.

Keywords: *Mobile money; mobile money systems; mobile network operators; mobile money service providers; security issues; Kenya.*

I. INTRODUCTION

The rapid growth of the FinTech industry and the increasing adoption of mobile money transactions have raised concerns about the security and safety of financial transactions in Nairobi. As mobile money services become more prevalent, ensuring the protection of user identities and securing these transactions becomes crucial. Identity Access Management (IAM) frameworks play a vital role in safeguarding the integrity, confidentiality, and availability of mobile money transactions. This research focuses on evaluating the effectiveness of IAM frameworks in ensuring the safety of mobile money transactions used by FinTech companies in Nairobi.

A. Background

The increased use of powerful mobile devices such as smartphones has transformed how users access financial services such as mobile money and banking. As a result, many third world nations have embraced mobile money transaction services as a potential money transaction platform. Mobile money transaction is defined as a wide scope of financial services accessible on a mobile phone. This service allows customers to get access to financial services by using mobile devices and dialing unstructured supplementary service data (USSD) codes. According to the Global System for Mobile Communications (GSMA), mobile money is now available worldwide with most lower and middle-income countries already onboard.

The evolution of the first mobile money services in the world can be traced back to 2001 with its inaugural deployment in the East African region taking place in Kenya when Safaricom launched M-Pesa in March 2007. This was later launched in Tanzania as M-pesa by Vodacom Tanzania in April 2008 and Z-Pesa by Zantel (Baganzi, R.; Lau, A.K, 2017). For Uganda, Mobile Telephone Networks (MTN) launched its first mobile money service in 2009, following the successful launch of M-Pesa in Kenya.

Since then the financial sector ICT has been influential in enabling financial institutions in extending its services through financial inclusion of people unreachable by these services and diversifying its services (Pilat, Lee & Van Ark 2003). Due to the dependency of digital technology companies are bound to go digital so that they have a better competitive edge as both businesses and financial institutions. This dependency has led to the advancement of digital technology extensively unfortunately, with little on the safety of mobile money transaction.

Banking services have been a key infrastructural pillar of the society. They not only offer financial governance, guidance, and benefits, but they also significantly streamline the fundamental trade exchange process. The idea of banking services has evolved over time to encompass a wide range of independent payment processing actors/institutions as well as those made possible by technology. This expansion goes beyond the traditional notion of established financial institutions like banks, credit unions, mortgage companies, pension funds insurance firms, and investment banks. Due to infrastructure issues, a sizable portion of the people in the emerging world did not have access to traditional banking services.

ISSN No:-2456-2165

Benefits of banking services such as macro and micro credit infrastructure, ease of money transfer and financial advisory had remained largely unavailable to the unbanked. This situation inspired the need for alternative considerations and this has tremendously changed with the evolution of FinTech and mobile money transfer.

These services are made available to the banked and unbanked mobile subscribers include mobile payments, mobile transfers and in some cases, mobile banking. They facilitate customers to create a (virtual) mobile money account, deposit funds into this account, make transfers and withdraw cash value in a manner that is secure, easy and cheap. Mobile money represents a synergy of two industries that have erstwhile existed independently – mobile telecommunications and financial services.

The most profitable market for FinTech executives is Kenya. According to a research by the Digital Frontiers Institute, Kenya is the most attractive African market for top FinTech executives, outpacing Nigeria, Tanzania, and South Africa in terms of monthly pay, which range from $12,000 to $20,000 at the upper end of the market. The market in Kenya is expanding as more SMEs implement cutting-edge financial technology solutions to reach an audience of consumers who are becoming more tech-savvy. This is supported by research conducted by Asoko Insight research analyst Levi Obingo. The FinTech environment in Kenya is thoroughly examined, with the top firms by subscription growth being examined along with the SME ecosystem, transaction values, transfer volumes, and other factors on the leading platforms in the sector.

According to data from the Kenya Bureau of Statistics (KBS), 49.3% of SMEs have mobile money and mPOS infrastructure in place in 2016, while 40% of SME owners had commercial mobile applications. Only 29% of SMEs were registered pay bill/till users.

However, mobile money transaction services rely on the acquisition and generation of huge individual data, both personal and non-personal. When done effectively, this data can boost efficiency in the operation of mobile money services by improving fraud detection mechanisms, and hence improved safety of mobile money transaction services by FinTech companies. The mobile money industry knows the value of responsible use of data and that this can lead to important changes to traditional ways by driving far reaching impact through improved access, chances and new opportunities for increased financial access. In the context of mobile money transaction services, responsible use of data by FinTech companies is critical to ensuring that the consumers of these services have sufficient control over their personal data. With this in mind, consumer data protection remains an important focal point for mobile money transaction, as they come to terms in understanding the need and the critical role is to empower individual consumers and protect their personal data in this advanced digital age.

FinTech allows its users to conduct financial transactions through mobile devices such as mobile phones and tablets. It is a service offered by banks and other financial institutions that allow users to obtain account balances, pay bills and transfer funds on their mobiles whereas FinTechis a service that allows users to pay for a product or service using a mobile device. Paying for purchases does not require having a bank account as it is more often paid in cash to specific agents across an area. As banks and other financial institutions take advantage of mobile, cloud, social and other technical trends to reignite growth and rebuild customer trust, several competing forces come into play: the need to innovate quickly, decrease IT complexity and deliver an unparalleled customer experience – all while providing the airtight security and digital privacy that customers expect. Against a backdrop of constant change, cloud, mobile and emerging technologies provide a foundation for innovation in products and services that support increased productivity and broader operational capabilities (Dattani, Ilesh. 2016).

In the same length, cyber criminals are also using this technology to launch increasingly damaging attacks such as Cloud based botnets that takeover processing power, exploitation of Near Field communications, which banks are using for new services, Distributed Denial of Service (DDoS) attacks launched via the cloud, thereby increasing their intensity and impact and Hacks on multifactor authentication technologies, fostering disruption and fear among customers.

As new mobile technologies expand the attack surface, attacks continue to grow rapidly. Android banking Trojans, such as the Android. iBanking Trojan, specialize in stealing banking information by intercepting SMS messages and continue to make the rounds. Email remains a significant attack vector for cybercriminals, but there is a clear movement toward social media platform. In 2014, Symantec observed that 70 percent of social media scams were manually shared. These scams spread rapidly and are lucrative for cybercriminals because people are more likely to click on something posted by a friend. Unwitting insiders who are the most cited culprits of cybercrime. (Dattani, Ilesh. 2016).

Many times, they unknowingly compromise data or jeopardize information security by circumventing security practices in favor of productivity or through the loss of mobile devices. Equally concerning, employees lacking a security mindset can easily fall victim to targeted phishing schemes. Not to be overlooked is the risk that third parties bring to the table. In today's interconnected business ecosystem, the security posture of partners, vendors and other critical third parties can have a tremendous impact on the risk posture of today's financial service firms. A holistic approach then is needed from when the need is required by the customer to make FinTech services readily available on mobile devices. I agree with the Dattani, Ilesh. 2016 where there is a need to innovate quickly, decrease IT complexity and deliver an unparalleled customer experience.

ISSN No:-2456-2165

However, all FinTech services projects undertaken by the FinTech companies should have an agile approach which would give guidelines on changing technology, customer experience and response to cyber incidents differently as per compared to the traditional way of software development. This is not captured by Dattani on how to develop the platforms and services with an agile mindset focusing on the customer collaboration and DevSecOps in the background.

As mentioned earlier despite the many benefits in improving access to financial services, there still exists security issues and challenges associated with the access management and maintenance of consumer data and information to prevent attacks through phishing, impersonation and all aspects of identity authentication. There has been few research done on security of mobile money, particularly in Africa, India, and South America, the safety of mobile money transaction by Fintech Companies particularly on identity access management and maintenance has not been surveyed in Kenya. The studies that were examined in this area include Mtaho [7] that investigated the security challenges associated with the mobile money authentication methods in Tanzania. Castle et al. [8] assessed the security challenges of mobile money in the developing world. Bosamia [9] identified and analyzed the different threats and vulnerabilities of a mobile wallet application. Additionally, this paper focused primarily on identity access threat on safety of mobile money transaction by Fintech Companies in Kenya.

The findings of this study will help the mobile money operators, mobile money decision-makers, and the government to identify and evaluate the key security issues associated with the safety of mobile money transaction in Fintech companies and recommendations proposed to address the security gaps.

B. Statement of the Problem

The safety of mobile money transactions in Fintech companies in Nairobi, Kenya is the problem we are facing. According to Demystifying the cyber security poverty line in Africa 2017 Cyber Security Report, most organizations, especially SMEs, are having difficulty putting in place the most fundamental identity access mobile money transaction safety mechanisms. More than 95% of African businesses, including public and private, are either operating at or below the "Security poverty line."

Cybersecurity risks to the financial system have grown in recent years, in part because the cyber threat landscape is worsening; in particular, cyberattacks targeting financial institutions and mobile money transactions are becoming more frequent, sophisticated, and destructive. In 2017, the G20 warned that cyberattacks could “undermine the security and confidence and endanger financial stability.”

As recorded by Carnegie’s Technology and International Affairs Program which keeps updates with timeline data provided by the Cyber Threat Intelligence unit of BAE Systems, it gives the following instances of cyber-attack on financial institutions. On February 4, 2022, researchers reported that the Medusa Android banking Trojan had increased infection rates and the scope of geographic regions targeted. The malware aims to steal online credentials to go on and perform financial fraud. Medusa had begun targeting victims in North America and Europe, using the same distribution service as FluBot malware to carry out their smishing (mobile text messaging) campaigns.

From May to August 2021, researchers from Cyren reported a 300% increase in phishing attacks targeting Chase Bank. The phishing kits were designed to mimic the Chase banking portal. This phishing kits were highly sophisticated and designed to harvest more than just email addresses and passwords, including banking and credit card information, social security numbers, and home addresses.In August 2019, the UN Security Council Panel of Experts indicated DPRK-affiliated actors were behind the attempted theft and in January 17, fraudsters stole Sh29 million from the National Bank of Kenya. The bank has noted that the attempted fraud was frustrated by the system's monitoring and security platforms, and that they were confident they could recover the siphoned funds.

With all this development in the FinTech sector, a new report by Levi Obingo from Asoko Insight shows that many large organizations are placing a greater emphasis on the resilience of their operational infrastructure and cyber security as a result of a number of system failures in 2017. During the 2017 holiday season, a problem with CBA's M-Shwari system prevented 17,700 users from accessing funds and resulted in delays of 72 hours. 3.21 million Users of Co-operative Bank's Mco-op Cash's mobile banking system experienced disruption. In April 2017, 28 million Safaricom customers and 100,000 M-fanisi users had similar issues.

Up to 41% of Kenyan enterprises lacked a functioning cyber-security program, according to a 2018 PwC research on global economic crimes, providing possibilities for would-be cybercriminals. This thus emphasizes the need for robust security measures in the country.

From the above studies, it therefore follows that, Identity Access Management (IAM) frameworks play a critical role in ensuring the security and privacy of mobile money transactions conducted by FinTech companies in Nairobi. With the increasing adoption of mobile money services in Kenya and the corresponding rise in cyber threats, it is essential to evaluate the effectiveness of IAM frameworks in safeguarding these transactions. However, limited research has been conducted specifically in the context of Nairobi's FinTech industry, leaving a gap in understanding the potential vulnerabilities and the need for improved IAM solutions.

ISSN No:-2456-2165

II. REVIEW OF RELATED WORKS

In the last dozen years' mobile technology has flourished throughout the developing world faster than any other technology in history. With this growth there has been equally an impressive surge of messaging services, providing not just a broadly used means of personal communications, but also a number of valuable information services. The latest entrant by mobile technology is mobile money transaction services. This trend is providing money transfer services to millions of previously not reachable people by banking services, facilitating sending money and paying bills.

Currently Kenya is among the global leaders in mobile money services, where mobile network operator Safaricom launched M-Pesa in 2007. After launch, there are approximately 16 million users of mobile money in Kenya, conducting millions of transactions every day. M-Pesa is not only being used for standard money transfers and airtime purchase, but also to pay salaries, utility and other bills, and to buy goods and services at both online and physical merchants. Three other mobile operators also followed and started to offer mobile money services in Kenya – Airtel, Orange, and Essar (Yu). Other players have recently emerged to offer complementary services. In addition, many FinTech companies and their implementing partners already begun to integrate mobile money into their programs and are at the forefront mobile money transaction.M-PESA is thus accredited with introducing financial services to low-income and unemployed persons across the country, unlocking economic opportunities for millions.

These mobile money transaction use USSD, short message services (SMS), and a subscriber identity module (SIM) toolkit (STK) technologies to provide access to users (Mtaho&Mselle, L., 2014). Mobile money platforms involve several players and stakeholders such mobile money operators, banks or other financial institutions, regulatory institutions, agent networks, merchants and retailers, businesses, mobile money users, equipment manufacturers, and platform providers, who perform different roles and in turn gain distinct benefits from the mobile money ecosystem. Mobile money transaction is now widely used in many fields, including, business, finance, health, agriculture, and education. It offers an extensive range of services including deposit and withdrawal of money, transfer of money to other users, pay utility bills (like water, electricity, DStv), purchase airline tickets (Kumar, G.R., 2016) pay for goods in a store, Lotto and sports betting, save money for future purchases or payment, receive a salary, take a loan, receive state aid or pension, purchase insurance, purchase airtime and data bundles, make bank transactions, pay for school fees, and taxes.

These services are rapidly deployed across emerging markets as a key instrument in economic growth. Mobile money transaction by FinTech companies has come out as an important innovation with potential benefits. For instance, it enhanced access to financial services for a large number of people who cannot access banks. According to Mwangi and Kasamani 2017, Murendo et al. 2018, and Saxena et al. 2019, mobile money transaction system provides a convenient way to send money to anyone who owns a mobile phone or has access to the mobile money agent. Nyaga 2015 mentioned that mobile money services include the reliable saving option for many low-income earners, reduction in loss of sales, good audit trail, and quicker transaction than cash at the point of sales.Kyeyune, Mayoka, and Miiro assert that the system is more secure since the money is not on a user's SIM card but a central server which I tend to disagree with as the modern era technologies has brought with enormous security concerns. Marumbwa and Mutsikiwaadded that mobile phones have brought massive opportunities in the provision of financial services. Mobile money services have enhanced the standard of living of people who cannot access bank and has led to the stimulation of economic development. Jack and Suri 2011, acknowledge that mobile money systems allow people to keep their savings hidden from friends or relatives who might ask for money. Mobile money transaction systems also greatly cut down the expenses and time lags associated with opening, operating, and maintaining a traditional bank account. Mobile money provides the quickest mechanism for clearing unplanned domestic financial payments. Successful mobile money deployment has led to the development of mobile commerce in the developing world. According to Maitai and Omwenga, mobile money transfer services have transformed the way the financial service industry conducts business where customers can access any time. Cisco, 2012, asserted that mobile money transfers are cheaper than electronic transfer services and more reliable than physically transporting money. Mobile money enables small and medium-sized enterprises (SMEs) to receive and make payments instantly through mobile phones and improves business networking. Additionally, mobile money leads to economic development through increased savings and investments.

III. RESEARCH DESIGN AND METHODOLOGY

This study employed a mixed-methods research design, combining quantitative and qualitative approaches. The quantitative phase involved data collection and analysis to evaluate the performance and effectiveness of Identity Access Management (IAM) frameworks in safeguarding mobile money transactions whereas the qualitative phase provided deeper insights into the challenges, user experiences, and potential improvements of IAM frameworks in the context of Nairobi's FinTech industry (Gay &Airasian, 2003).

The target population consisted of FinTech companies in Nairobi that offer mobile money services. The population was identified through existing databases, industry directories, and partnerships with relevant organizations. It involved different departments of IT and cyber security, as they are the first line of defense from the attackers. The IT included Cyber analysts, system administrators, IT administrators, database administrators and IT support teams. Majority of companies had a team of approximately 5-20 cybersecurity analysts who were used as the sample size.

ISSN No:-2456-2165

A sample of SOHO users' data was gathered. A SOHO business is one with fewer than ten or more than one hundred employees (Gupta et al., 2013). Due to the limited number of cyber security team members, the sample size was determined to avoid superficial, one-sided, and unsupported data as well as to obtain workable data from the general public by purposive sampling. Thus purposive sampling technique was used to select a representative sample of FinTech companies. The selection criteria included factors such as company size, market share, and technological capabilities. The sample size will be determined based on data saturation and the principle of adequacy, ensuring sufficient information for analysis.A sample size of 80 respondentswas determined using Slovin's formula;

$$n = \frac{N}{1 + N^* (e)2}$$

n – the sample size
N – the population size
e – the acceptable sampling error
95% confidence level and p = 0.5 are assumed
When this formula is applied to the sample

$$n = \frac{100}{1 + 100\ (0.05)2} = 80$$

Both primary and secondary data was gathered for this project. After describing the study's purpose, participants were asked for theirwillingnes to participate in the study as part of the data collection process.Questionnaires and personal interviews were used as the primary source of information. A draft of general cybercrime related questions were asked regarding FinTech to get the best feedback for analysis. Interviews were used to enforce the Questionaries' process as they could both be conducted concurrently during the data collection process. Documents reviews, publications, journals, reports, and online repositories were used to enforce the primary data collected. Online research was also used to collect secondary data.

The questionnairefor both qualitative and quantitative data on a five point Likert Scale rating was designed to capture information on IAM framework features, security measures, and transaction performance forming was analyzed using descriptive statistics inferential statistics respectively. Qualitative data was analyzed using inferential statistics and content analysis. Results highlighted.

Descriptive data was summarized, while inferential statistics, such as correlation analysis and regression analysis, was applied to examine relationships between variables and identify significant factors affecting IAM framework performance.

IV. RESEARCH FINDINGS AND DISCUSSION

This section presents the research findings and discusses the results of evaluating Identity Access Management (IAM) frameworks on the safety of mobile money transactions used by FinTech companies in Nairobi. The section covers research respondent's general information and a discussion on the (IAM) framework findings. The findings provide insights into the effectiveness of IAM frameworks, challenges faced, and potential improvements to enhance transaction security.

A. General Information

From the results of the study the ages of the respondents ranged from 18years to 50 years with the majority being 25-38 years and the highest age being 28years of age at 11.1% followed by 25years, 35years and 38 years who all stood at 7.4%.

On the level of education, majority of the respondents had a bachelor's degrees at 77.8%, and 20.4% for respondents with a post graduate degree, then other professional certificate at 16.7% then followed by Certificate and Diploma at 3.7% and 1.9%. This implies that most of the Fintech companies' employees are literate with a high level of education.

The researcher also sought to find the number of years the respondents had worked in both ICT and Cybercrime departments. This pushed the understanding of the IT for easy mastery of the cybersecurity domain where prevention is key. The findings revealed that most of the respondents had a range of 3 to 8 years of experience in the IT domain. The highest of the respondents being 22.2% having worked for 3 years then followed by 4 years of experience at 14.8% and a tie of 9.3% being 5 and 8 years of experience.On number of years worked in the cybersecurity domain, the majority of the respondents at 32.7% had 1year or less of experience then followed by 23.1% had 2 years of experience. This shows the growing demand of cybersecurity experts in Fintech.

B. Identity Management and Access Control Framework

The study sought to find out how identity management and access control framework affected the safety of mobile money transaction in Fintech companies. The researcher looked at the following aspects, one whether credential verification and revocation are audited on user and two, whether the maintenance framework where company IT assets should be approved and logged.

On credential verification the respondents were asked to indicate the extent to which physical access was managed on assets, remote access was managed, all user and device authentication, credential verification and the extent to which network segmentation and segregation was managed. The results are as presented in the graphs below;

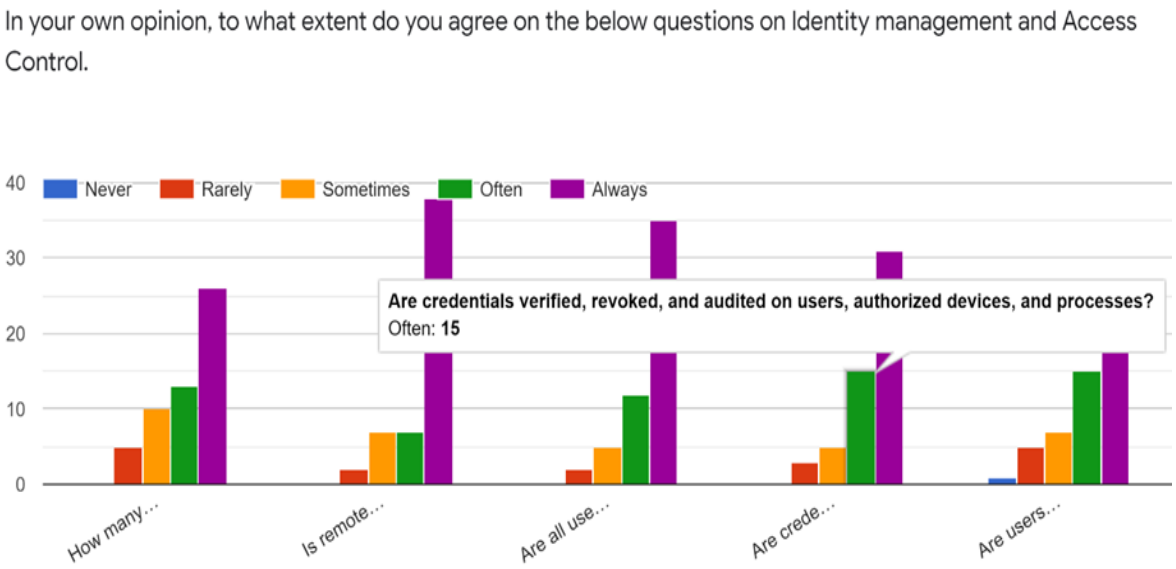

Fig. 1:

The results displayed in figure 1 first graph shows the extent to which physical access managed on assets. 48.1% of the respondents are the majority recording Always followed by 22.2% recording Often. This is followed by 18.5% of the respondents who recorded, Sometimes, 9.3% as Rarely and lastly 0% recorded Never.

The second graph of figure 1 shows the extent to which is remote access is managed. 68.5% of the respondents are the majority recording Always followed by 13% recorded Often followed by 13% recorded Sometimes followed by 3.7% as Rarely and lastly 0% recorded Never.

The results displayed in figure 1 third graph shows the extent to which all users and devices authenticated as per your policy. 64.8% of the respondents are the majority recording Always followed by 22.2% recorded Often followed by 7.4% recorded Sometimes followed by 3.7% as Rarely and lastly 0% recorded Never.

The fourth graph shows the extent to which credentials are verified, revoked, and audited on users and devices. 57.4% of the respondents are the majority recording Always followed by 27.8% recorded Often followed by 9.3% recorded Sometimes followed by 5.6% as Rarely and lastly 0% recorded Never.The results displayed in figure 1 fifth graph shows the extent to which both network segmentation and segregation managed well to promote network integrity 48% of the respondents are the majority recording Always followed by 27.8% recorded Often followed by 13% recorded Sometimes followed by 9.3% as Rarely and lastly 1.9% recorded Never.

C. Inferential Analysis

The study sought carry out correlation and regression analysis of the study variables. Thus, he applied Pearson correlation analysis to examine the strength, of the relationship between identity access management and maintenance and the safety of mobile money transactions in FinTech companies in Nairobi. The analysis revealed that there was a positive and a significant relationship between as illustrated in the following segments.

D. Identity Management, Authentication, Access Control Framework

The bivariate linear regression analysis results for Identitymanagement, authentication, and access control framework on the safety of mobile money transaction in FinTech Companies in Nairobi is as shown in Table 4.5 to 4.7.

Table 1: Model Summary for Identity Management

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.221[a]	.490	.031	.948	.490	2.731	1	53	.000

a. Predictors: (Constant), Identity Management

According to Table 1's regression results, the R value was 0.221, demonstrating a favorable correlation between the security of mobile money transactions in Nairobi FinTech companies and identity management, authentication, and access control framework. The identity management, authentication, and access control framework account for 49.0% of the safety of mobile money transactions, according to the R squared (R2) value of 0.490, all other parameters being held constant. The remaining 51.0 percent is explained by other factors.

ISSN No:-2456-2165

Table 2: ANOVAResults for Identity Management

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.455	1	2.455	2.731	.000[b]
	Residual	47.654	53	.899		
	Total	50.109	54			

a. Dependent Variable: Safety of mobile money transactions
b. Predictors: (Constant), Identity Management

The model's F ratio was significant at 2.731 at a p-value of 0.000 to 0.05. This shows that Nairobi-based FinTech companies believed the identity management, authentication, and access control framework to have a major impact on the security of mobile money transactions.

Table 3: Regression Coefficient for Identity Management

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	5.216	.553		9.433	.000		
	Identity Management	.212	.128	.221	1.653	.104	1.000	1.000

a. Dependent Variable: Safety of mobile money transactions

Identity management, authentication, and access control framework had positive and significant effect on safety of mobile money transaction in FinTech Companies in Nairobi with $\beta = 0.212$ at p value 0.000 which is less than 0.05. From Table 4.7, the bivariate linear regression model equation fitted using unstandardized coefficients is $Y= 5.216 + 0.212X1 + e$ where 5.216 is the constant and X1 is Identity management, authentication, and access control framework index. This means that Identitymanagement, authentication, and access control framework positively and significantly influence safety of mobile money transaction in FinTech Companies in Nairobi. It also means that an increase of one unit of X1 increases Y by 0.212. The indication was that Identity management, authentication, and access control framework is a major factor on safety of mobile money transaction in FinTech Companies in Nairobi.

V. SUMMARY

The study sought to evaluate the Identity Access Management Frameworks on the safety of mobile money transactions used by FinTech companies in Nairobi. On the pertinent IAMF research components the responses were as follows; Most of the respondents indicated that they always manage remote access, they manage physical access of assets, authenticate all users and devices as per policy, and manage both network and segregation which promotes network integrity.

On the credentials being verified, revoked, and audited on users and devices majority of the respondents always checked the credentials. As this is being done it was also evident that access permissions and authorizations are managed, incorporating the principle of the least privilege ad separation of duties. Lastly the respondents indicated that they always check the users and devices authentication in proportion with the risk of the transaction plus they always check the extent number of times which identities are proofed and bound to credentials with the required interaction. This is in line with the work of Trulioo (2015) and Mtaho (2015) who noted that identity theft is usually an inside job activity through unscrupulous employees gaining unauthorized access to mobile money data that belongs to the users and then irregularly misappropriating their funds. This is affirmed by Gwahula (2016) who observed that identity theft results from fraudulent or offline SIM swaps by fraudsters that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, enabling them to have full access to the user's mobile wallet to carry out fraudulent transactions. Thus, the need to always maintain the remote working of the Fintech company assets approval, logins performed in a preventive manner as indicated by most respondents. It was also noted that a high number of respondents always maintain and repair the company IT assets which are approved and logged.

VI. CONCLUSION

As noted in the study mobile money transactions plays a major role as the primary payment platform for the digital economy, hence improved standards of living of many people with limited access to the banking infrastructure in third world nations like Kenya. By enabling access to cashless payment infrastructure by FinTech companies, this infrastructureenables individuals to decrease the physical security risks associated with hard currency transactions. However, the safety of mobile money transactions remains a big challenge. In this paper, the researchers evaluated theidentity access management and maintenance on the safety mobile money transaction by Fintech companies in Kenya. They found significant security challenges with the current mobile money transactions such as identity theft, authentication attack, phishing attack, vishing attack, SMiShing attack, PIN sharing, and agent-driven frau. Several recommendations for successful and improved safety of mobile money transaction such as the implementation of better access controls, customer awareness campaigns, agent training on acceptable practices, high-value transaction monitoring by FinTech companies among others. The findings of this paper contributes to research in many ways which include; extending the theoretical knowledge of safety of mobile

money transaction by FinTech companies. The study also offers meaningful managerial contributions and suggests by identifying and improving the safety issues and challenges of mobile money transactions thus important in the implementation of secure mobile transaction services. This study encountered some limitations that create an opportunity for future research on mobile money systems' security challenges.

VII. RECOMMENDATIONS

The study recommends that for safety of mobile money transaction for FinTech companies through identity access and maintenance FinTech should follow the NIST framework. The framework has been adopted by many Fintech companies as per the respondents. It was very clear that the identity management and Access control frameworks was highly adopted for better protection. On awareness and training framework the respondents had an issue with third party stakeholders who include suppliers, customers, partners who a high number of them not fully understanding their roles and responsibilities. This can be a loophole and can be used by to attack mobile money transactions Fintech should have a clear policy that enhance understanding of roles and responsibilities where the third-party stakeholders fully safeguard themselves within the FinTech Platforms.

Also, constant awareness using different and more agile methods of spreading the awareness fully can go a long way for the third-party stakeholders to be aware of their roles and responsibilities. On the data security framework, it was evident that most of the respondents adhered to the NIST framework. It was noticed that a percentage of assets are formally managed throughout the removal, transfer and disposition were on the 50% -69% category. Fintech should enforce the above to increase the percentage either by having a system that manages the assets and followingset guidelines of removal, transfer, and disposition regardless of the size and age of the equipment. Spot checks and regular audits on the management system or process should be done to check on how the assets are handled will assist greatly on safeguarding the mobile money transactions in FinTech. Management should invest to have a separate environment for production, development, and test. This enhances security as vigorous tests can be done on the test environment separate from the development environment.

The security management team should focus on implementing integrity checking mechanism that are used to verify hardware integrity this will enhance security. Another integrity checking mechanism that the management should put in place is the one that verifies software, firmware, and information integrity. In case of any anomaly protection can be enforced to avoid any cyber-attacks on the mobile money transactions. On information protection processes and procedure framework management should focus on enforcing how data is destroyed according to policy. If some data isn't destroyed according to the laid down policy, then this provides a loophole on the security of the mobile money transactions.

Response and recovery plans should be tested from time to time in the event of a cyber-attack; the timeframe can be determined by management. Cybersecurity should be included more in the human resource screening as a precaution to vet onboarding or leaving staff from the Fintech companies. On the protective technology framework management should enforce auditing of logs documenting, implementing, and reviewing them in line with the laid policies. The management should also put more mechanisms in place like hot swap, load balancing and failsafe to achieve resilience in all situations. The management should also factor in the principle of least functionality used on systems to provide essential capabilities to be used.

ACKNOWLEDGEMENT

I would wish to acknowledge my research supervisors, Dr. BonfaceRatemo PhD, and Dr George Musumba, PhD, DedanKimathi University of Technology for the professional guidance they have accorded me during my journey of writing this paper.

REFERENCES

[1.] Abu-Shanab, E., &Matalqa, S. (2015). Security and Fraud Issues of E-banking. *Int. J. Comput. Netw. Appl*, *2*, 179-187.

[2.] Baganzi, R.; Lau, A.K. Examining Trust and Risk in Mobile Money Acceptance in Uganda. Sustainability 2017, 9, 1–22.

[3.] 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.

[4.] Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. ABC-CLIO.

[5.] 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.

Otieno, E. O., &Kahonge, A. M. (2014). Adoption of Mobile Payments in Kenyan Businesses: A case study of Small and Medium Enterprises (SME) in Kenya. *International Journal of Computer Applications*, *107*(7).

[6.] Dattani, Ilesh. (2016). Financial Services and FinTech - A review of the Cyber Security threats and implications.

[7.] Gregory, L., & Charles, E. (2015).Cyber criminology, Criminology and Cybercrime: Towards an Academic Discipline.

[8.] Gwahula, R. Risks and Barriers Associated with Mobile Money Transactions in Tanzania. Bus. Manag. Strategy 2016, 7, 121–139.

Hove, L.V.; Dubus, A. M-PESA and Financial Inclusion in Kenya: Of Paying Comes Saving? Sustainability 2019, 11, 568. [CrossRef]

[9.] Intelligence, G. S. M. A. (2017). The Mobile Economy: Sub-Saharan Africa 2015. 2015.
[10.] IOSR J. Econ. Financ. IOSR-JEF 2015, 6, 2321–5933.
[11.] Jaishankar, K. (2007) International Journal of Cyber Criminology Vol 1 Issue 2 July 2007. Retrieved from http://www.cybercrimejournal.com/Editoriaijccjuly.pdf
[12.] Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., & Siyanda, S. (2015). *Kenya Cyber Security Report 2015*. Serianu Limited.
[13.] Kyeyune, R.; Mayoka, K.G.; Miiro, E. ICT Infrastructure, Mobile Money Systems and Customer Satisfactionin Uganda. Int. Sci. Res. J. 2012, 1, 1–8.
[14.] Maitai, J.; Omwenga, J. Factors Influencing the Adoption of Mobile Money Transfer Strategy in
[15.] Mtaho, A.B. Improving Mobile Money Security with Two-Factor Authentication. Int. J. Comput. Appl. 2015, 109, 9–15
[16.] Murendo, C.; Wollni, M.; De Brauw, A.; Mugabi, N. Social Network Effects on Mobile Money Adoption in Uganda Social Network Effects on Mobile Money Adoption in Uganda. J. Dev. Stud. 2018, 388, 1–17.
[17.] Njoroge, E. W. (2018). *Effect of Cyber Crime Related Costs On Development of Financial Innovation Products and Services* (Doctoral Dissertation, Jkuat-Cohred).
[18.] Nyaga, J.N.; Ogollah, K. Challenges Facing Penetration of New Mobile Money Transfer Services in Nairobi.
[19.] Organisation for Economic Co-operation and Development. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. OECD Publishing.
[20.] Pilat, D., Lee, F., & Van Ark, B. (2003). Production and Use of ICT. *OECD Economic Studies*, *2002*(2), Durkheim, E. (2018). The division of labor in society. In *Inequality* Routledge.
[21.] Saxena, S.; Vyas, S.; Kumar, B.S.; Gupta, S. Survey on Online Electronic Payments Security. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019; pp. 746–751
[22.] Subia, M. P., & Martinez, N. (2014). Mobile Money Services: A Bank in your Pocket—Overview and Opportunities. *ACP Observatory on Migration, Brussels*.
[23.] Telecommunication Industry in Kenya: A Case of Safaricom–Kenya Ltd. IOSR J. Bus. Manag. IOSR-JBM 2016, 18, 84–94. [CrossRef]