Curbing Mobile Phone Terrorism and Financial Fraud: A Kenyan Perspective

Philip Muriuki Wanjohi

Kirinyaga University, Kenya
E-mail: philipwanjohi2002@gmail.com

Received 19 December 2016;
Accepted 8 March 2017

Abstract

Kenya being a leading mobile phone operator in Africa provides a suitable platform of understanding security weaknesses in relation to terrorism and financial frauds perpetrated through mobile phone technology. According to [5]; origin and use of mobile money transfer make the country a suitable case that can be replicated elsewhere in the world. It is worth noting that growth of mobile money transfer has promoted business alongside creating new employment opportunities in Kenya. However the growth of mobile phone technology has had an equal share of problems; subsequently leading to challenges of financial frauds, and terrorism activities. This paper addresses a mechanism of safe mobile phone technology through enhanced biometrics during financial transactions, SIM registration, and forensic audit trail in case of a crime.

Keywords: Alshabaab, Agent, Biometric, M-pesa, Safaricom, Sim.

1 Background of the Study

From a study which was carried out by [5]; it was found that most people in Kenya are able to afford mobile phone handsets. As indicated in Table 1; the study found that 78.8% and 94.6% of respective rural and urban populations in Kenya had mobile phone handsets.

Journal of ICT, Vol. 4_3, 237–246.
doi: 10.13052/jicts2245-800X.434

Table 1 Percentage of people with mobile phone, in Kenya. Source: [5]

	Rural	Urban	Total
No	21.2%	5.4%	16.1%
Yes	78.8%	94.6%	83.9%
Total	100.0%	100.0%	100.0%

The study further indicated that 83.9% of Kenyan population was able to consume mobile phone technology and within a short span. The study by [5] is also in agreement [11] who indicated that the adoption of mobile phones technology was fastest when compared with other technologies in the history of mankind. This makes Kenya no different from the rest of the world. Figure 1 below is a comparison of technology adoption by mankind in the world and mobile phone technology leads.

In Kenya; mobile phones are mainly used for communication and financial transactions. Financial transactions are mainly carried out using mobile phones and through a program called M-pesa. According to [9] M-pesa was developed by mobile phone operator Vodafone and launched commercially by its Kenyan affiliate Safaricom in March 2007. M-pesa ("M" for mobile and "pesa" for money in Swahili) is an electronic payment system through mobile phones. To access the service, customers must first register at an authorized M-pesa retail outlet. They are then assigned an individual electronic money account that is linked to their phone number and accessible through a sim card-resident application on the mobile phone. Once customers have money in their accounts, they can use their phones to transfer funds to other M-pesa users.

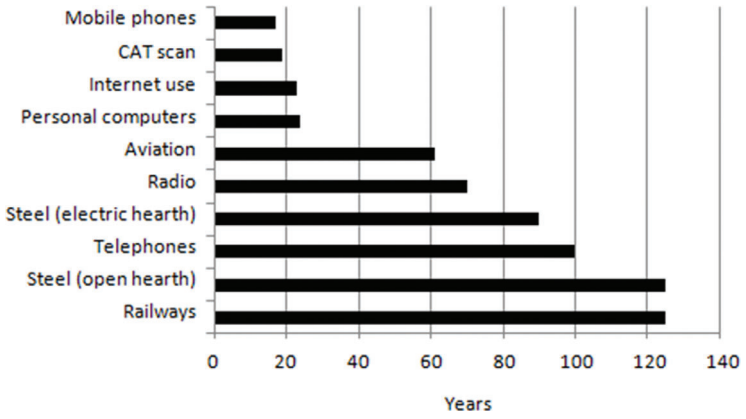

Figure 1 Technology adoption for select innovations (number years to reach 80% coverage). Source: [11].

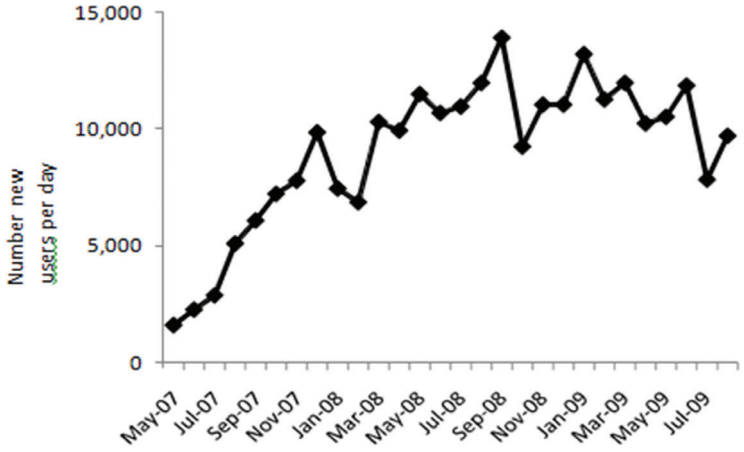

Figure 2 Average daily growth in M-PESA registrations by month. Source: [11].

As indicated by [11] M-pesa has spread quickly, in Kenya and has become the most successful mobile phone-based financial service as demonstrated in Figure 2.

As indicated in Figure 2 above; the average number of new registrations per day exceeded 5,000 in August 2007, and reached nearly 10,000 in December. By August 2009, a stock of about 7.7 million M-pesa accounts had been registered. Figure 2 above further indicates that 38 percent of the adult population in Kenya had gained access to M-pesa in just over 2 years.

1.1 Problem Statement

The statistical figures in Table 1, Figures 1 and 2 suggest that most Kenyans can afford to quickly acquire a mobile phone for use. Once a mobile phone is purchased; it becomes useful after being inserted with a sim (Subscriber Identification Module) card and credit purchased for purposes of communication. According to [7] of the Kenya Government it is illegal to use a mobile phone sim card without having the details of the user registered by the respective mobile phone provider. However many cases continue being reported about criminals who use multiple sim cards for financial frauds and illegal communication. A case in point is a report by [2] where a raid was carried out on 6th January 2016 by the communication authority officers together with Kenya police on an illegal facility in Nairobi. The officers recovered four sim box equipment (Sim-boxing involves termination of international traffic using illegal routes. The perpetrators use sim box devices,

which hold stacks of sim cards on one side and is connected to the Internet on the other side. Instead of international calls coming in through the traditional international gateways, these operators receive the calls through the internet and then using the sim box; re-originate the calls through the stacks of sim cards as if the calls are being originated by local customers). Also recovered, were a total of 5,827 illegal sim cards from the local mobile phone providers. In particular, the officers found 3,017 sim cards from Orange, 2,678 sim cards from Airtel, 52 Yu sim cards and 80 sim cards from Safaricom.

1.2 Knowledge Gap

An illegally obtained sim card is dangerous to the security of a country and its people. Criminals can use such cards to create communication networks which are not easy to detect. Forensic evidence is also difficult to come by after a crime has been committed. The solution to this problem is ability to identify genuine mobile phone users through biometrics processes like finger print scanning when buying sim cards; and during mobile financially transactions.

1.3 Objectives of the Study

i. To identify the limitation and loophole in SIM card registration in Kenya
ii. To establish the relationship between unregistered SIM cards and crime (terrorism and financial fraud)
iii. Propose a more secure SIM card registration model Bases on biometric identification

2 Literature Review

2.1 Registration Process of a Sim Card

According to Group Special Mobile Association [3]; sim card registration is mandated in a number of countries and it requires consumers to provide proof of identification in order to activate and use a mobile sim card. A number of governments adopt this policy as part of efforts to help mitigate security concerns and to address criminal and anti-social behaviour. [3] notes that registration exercise is implemented effectively by taking into account the ability of mobile operators to verify customers' identity documents. [3] further notes that sim registration can benefit many people access digital services that would otherwise be unavailable to them if unregistered. In agreement with Group Special Mobile Association the (Legal notice 163, 2015) of

Kenya directs that all telecommunication operators register sim cards of their subscribers. The above legal notice was published after alshabaab (a terror group from Somalia) terror attack in Westgate Nairobi in September 21, 2013, where more than 70 people died and more than 175 were injured. The terror attack was therefore a wakeup call to Government of Kenya on the impact of unregistered mobile phone sim cards. Thereafter; (Kenya National Assembly, 2013) released an inquiry report into Westgate terrorist attack, Mandera in north-eastern Kenya attack and Kilifi in the coastal region of Kenya attack. In the enquiry report the following was recommended:

i. Mobile phone companies need to comply with the law to ensure all sim card owners are duly registered.
ii. That there was need for collaboration with the security organs to ensure identification documents presented for registration were verified and authenticated as belonging to the applicant.

The enquiry report also noted the following:

i. That four Safaricom sim cards were recovered from the vehicle used by the terrorists who attacked Westgate Nairobi Kenya.
ii. That mobile communication was peculiarly disrupted on occasions when there were serious terrorism issues.
iii. Foreigners had acquired national IDs illegally, and were using them to launder wealth and perform other crimes.

In agreement with Parliament enquiry report; this study was able to establish that terrorists who attacked Westgate may have acquired Kenya national identification documents illegally, and consequently used the same to illegally buy and register mobile phone sim cards. Alternatively the terrorists exploited the lawful 90 days window time to own mobile phones. According to legal notice 2015; the procedure of registering Kenyan citizen for sim card issue involves the following:

i. An original identity card or
ii. An original and valid passport or
iii. An original service card for a member of the Kenya Defense Forces

For a foreign national the following is required:

i. An original and valid passport; or
ii. An original alien card.

The legal notice further continues to state that; if within ninety days a person fails to register identification particulars, the sim card shall be suspended and deactivated. This implies that it is lawful in Kenya of any person

(terrorists included) to be sold a sim card without any registration of documents and use it within the ninety days window time. This further implies that criminals can easily take the opportunity of the window time to use their mobile handsets for financial frauds and other terrorism activities.

Kenya Parliament enquiry report indicated that the government always disrupts mobile phone communication in areas that have been attacked by terrorist. This is a clear demonstration of government awareness of the link between terror and mobile phones. A study by [10] finds that there are two categories of sim card registration done to enable frauds and which are:

i. People who use fake registration documents to obtain sim cards. The sim cards are later used to do financial transaction.
ii. People who obtain genuine registration documents fraudulently and later use them to register their Sim cards.

It is these same types of sim ownership that [1] also finds responsible for fraudulent financial transaction in his study. Though registration of sim card owners continue in Kenya irrespective of the security challenges and financial frauds; [3] notes that secure and authorized digital identity is becoming increasingly important in most countries to enable people access digital services. The author indicates that mobile phone sim registration if done honestly would provide the best platform to deliver this. Unfortunately as indicated in the Parliament terror enquiry report it is not possible to do so in Kenya without registering dishonest people. [3] notes that mobile phone platform could significantly help in meeting the United Nations Sustainable Development Goal target 16.9: "free and universal legal identity, by 2030". This could be so in Kenya if other ways of identification were explored during sim registration.

2.2 Mobile Money Transfer

Mobile money refers to a diverse set of services that involves accessing financial services and performing transactions via mobile devices. The financial transactions may be handled using existing payment instruments (e.g. bank account, debit and credit cards, service provider's billing account, etc). Consequently; there is a wide range of activities in Kenya within today's telecommunications environment that fall under the term M-pesa. Some of the most popular are:

i. Mobile-to-mobile money transfers
ii. Applying cash to mobile phone for transfer to a bank account

iii. Transfer of funds from a bank account to a mobile account
iv. Transfer of funds from bank account to another bank account

All the above transactions are not possible when one does not have a sim card and a mobile phone. However evidence available from [2] Kenya police, and Kenya parliament indicate possibility of owning an illegal sim card in Kenya. An illegal sim card is equal to a legal sim card in carrying out M-pesa transactions and making phone calls. Below are the steps involved when legally registering a Safaricom sim card for phone calls and M-pesa business.

i. Buy a sim card from authorized Safaricom outlet or from a street hawker.
ii. Fill the sim card and personal identification details on a Safaricom registration form available at Safaricom outlet; or from street hawker who has been appointed by Safaricom.

The above procedure as stated by Safaricom has no provision of authenticating the personal identification documents used for sim registration. The above procedure by Safaricom leaves a huge security gap which can be exploited to register sim cards.

2.3 Personal Identity Card

The Kenya Government issues personal identification cards to Kenyans of eighteen years and above. The following are the security features found on personal identification card; a serial number, a unique identification number, finger print, and a facial photo. Mobile phone providers use the identity card to register subscribers. Mobile phone companies like other organizations and businesses extremely trust personal identification cards. As observed by [4] it is always easy to obtain a personal identification card details during a business transaction and thereafter make a counterfeit personal identification card. This implies that fake identifications cards can be used as a platform to make a fake sim registration with a purpose of hiding identity of users during crimes.

2.4 Westgate Terror Attack

Mobile phones as tools of terror was evidenced on CNN (Cable News Network) 9:55 AM Kenya Time, Thu October 17, 2013; terrorists were screened on the television strolling through Westgate mall, and with guns strapped to their torsos, the attackers chatted on their mobile phones while they sprayed bullets to terrified shoppers. The observation on CNN television demands that further studies be carried out to establish the following;

i. If the phones used by terrorists had sim cards.
ii. If the sim cards were registered in Kenya or in another country.
iii. If mobile phones transacted money in the popular M-pesa business.
iv. If the phones used local credit.
v. If the mobile phones communicated through the equipment of local mobile phone providers.
vi. If it was possible to track sim card numbers that called in and out of the mall and hence incidentally know their owners.
vii. If the terrorists were making calls to other terrorists in or outside Kenya.
viii. If the mobile phones found by police in the vehicle used by the terrorists were the same ones used when shoppers were getting sprayed with bullets.

Answering the above forensic questions would complement this study and also help the Kenya Government and the world to contain terrorism and other frauds.

2.5 Registration of Frauds in Kenya

With possibility of fake personal identification documents, this study concludes that there may be many people who have illegal sim cards which they use to do M-pesa transactions and communicate. This is further worsened when mobile phone companies puts integrity aside to allow any person to sell and do sim registration.

3 Methodology of the Study

This study used desk research method to obtain printed information from the libraries and the internet. There was no fieldwork done.

4 Proposed Recommendations

4.1 Use of Biometrics and Documents Authentication in Sim Card Registration

To control crime perpetuated through mobile phones, this study suggest that the following be done. All sim cards should be sold by a third party company. The third party organization should do the following before selling the sim card.

i. Check the authenticity of personal identification cards and passports by verifying them with registrar of persons and immigration
ii. Capture facial and finger print biometric details

iii. Keep all facial and finger print biometric details in a database,
iv. Share facial and finger print biometric details with all mobile phone companies in the country.
v. Mobile phone companies should activate a sim card to enable calling and money transfer after counter checking the same details with the third party organization.

All agents who transact business on behalf of mobile phone companies should use a computer and a finger print scanner which are wirelessly connected to the database of the mobile phone company. When a customer wishes to do money transfer, the finger print should be scanned at the agent's desk to authenticate his/her identity with the mobile phone company. Transactions with the mobile phone operator should therefore not be enabled if the person is not biometrically identified. If identified the mobile phone company will send an acknowledgement to both the agent and customer to proceed with the transaction.

5 Conclusion

As Kenyans address modes of curbing insecurity, financial frauds and terrorism facing the country, there is dire need of the security system of the country and researchers to address the methods used by mobile phone companies to register phone users. As indicated by [5] more methods should be explored to remove falsely registered sim cards from the society. This paper has focused on how to increase security and accountability through biometric sim registration, and authentication during money transfer. If the recommendations of this paper are implemented then it will be easier to have an audit trail in case of crimes involving a mobile phone. This study recommends that more study be done on forensic audit trail if crimes are committed through mobile phones.

References

[1] Adrian, D. (2016). *Mobile Phone Banking Usage Experiences in Kenya*. Nairobi: Catholic University of Eastern Africa.
[2] Communications Authority of Kenya (2015). *Mobile phone ownership Nairobi Kenya.* Available at: www.ca.go.ke (accessed March 10, 2017).
[3] Global System Mobile Association (2016). *The Mandatory Registration of Prepaid SIM Card Users.* London: Global System Mobile Association.
[4] Guizzo, E. (2006). Britain's identity crisis [biometric ID cards] Spectrum. *IEEE*, 43:42. doi: 10.1109/MSPEC.2006.1572352.

[5] International Telecommunication Union (2016). *Understanding Cybercrime: A Guide for Developing Countries Geneva Switzerland*. Geneva: International Telecommunication Union.
[6] Kenya National Assembly (2013). *Report of the Joint Committee on Administration and National Security; and Defence and Foreign Relations on the Inquiry into the Westgate Nairobi Terrorist Attack, and other Terror Attacks in Mandera in North-Eastern and Kilifi in the Coastal Region Government Printer*. Nairobi: Kenya National Assembly.
[7] Legal notice 163 (2015). *The Kenya Information and Communications Act*. Nairobi: Government Press.
[8] Guizzo, E. (2006). *Loser Britain's Identity Crisis*. Available at: http://spectrum.ieee.org/computing/software/loser-britains-identity-crisis (accessed October 24, 2016).
[9] Ignacio, M., and Dan, R. (2010). *Mobile Payments go Viral: M-Pesa in Kenya*. Washington, DC: World bank.
[10] Joseck, L. M. (2015). *Fraud in Mobile Financial Services*. Nairobi: A microsave publication.
[11] William, J. T. (2010). *The Economics of M-PESA*. Washington, DC: Georgetown University.

Biography

P. M. Wanjohi is an ICT assistant lecturer at Kirinyaga University in Kenya. He is also a student of Masters of Information System at Kisii University in Kenya. He attended Kampala University in Uganda where he received his B.Sc. in Computer Science and Information Technology in the year 2006. Philip Wanjohi will graduate any time soon at Kisii University. His interests centers on; use of mobile phones in developing countries, application programming, computer networks, data communication and web designing.