Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.8, No.6, 2018
www.iiste.org

Using Keystroke Dynamics and Location Verification Method for Mobile Banking Authentication.

Edwin M. Miiri* Dr. Michael Kimwele Dr.Ogada Kennedy
School of Computing and Information Technology (SCIT) Jomo Kenyatta University of Agriculture and Technology (JKUAT), PO box 62,000 – 00200, Nairobi, Kenya

Abstract
With the rise of security attacks on mobile phones, traditional methods to authentication such as Personal Identification Numbers (PIN) and Passwords are becoming ineffective due to their limitations such as being easily forgettable, discloser, lost or stolen. Keystroke dynamics is a form of behavioral biometric based authentication where an analysis of how users type is monitored and used in authenticating users into a system. The use of location data provides a verification mechanism based on user's location which can be obtained via their phones Global Positioning System (GPS) facility. This study evaluated existing authentication methods and their performance summarized. To address the limitations of traditional authentication methods this paper proposed an alternative authentication method that uses Keystroke dynamics and location data. To evaluate the proposed authentication method experiments were done through use of a prototype android mobile banking application that captured the typing behavior while logging in and location data from 60 users. The experiment results were lower compared to the previous studies provided in this paper with a False Rejection Rate (FRR) of 5.33% which is the percentage of access attempts by legitimate users that have been rejected by the system and a False Acceptance Rate (FAR) of 3.33% which is the percentage of access attempts by imposters that have been accepted by the system incorrectly, giving an Equal Error Rate (EER) of 4.3%.The outcome of this study demonstrated keystroke dynamics and location verification on PINs as an alternative authentication of mobile banking transactions building on current smartphones features with less implementation costs with no additional hardware compared to other biometric methods.
Keywords: smartphones, biometric, mobile banking, keystroke dynamics, location verification, security

1. Introduction

Authentication is the use of one or more mechanisms to confirm that you are the authenticated user claimed to be Asif *et al.* (2017) .In any given system faces challenges of threats and vulnerabilities. A threat may be defined in two ways: techniques that attackers use to exploit the vulnerabilities in your system components or impact of threats to your assets (Mouna *et al.* 2014).While vulnerabilities can be defined as flaws or weaknesses in system security procedures, design, implementation, or internal controls (Manal & Haydar 2016). Keystroke dynamics, refers to the typing pattern of an individual. Keystroke dynamics is one of the authentication mechanisms which uses natural typing pattern of a user for identification Ivannikova *et al.* (2017). Geo location is a term used to refer to the geographical location of the user, based on available information. Location can be used to authenticate users based on cookies, Global Positioning System (GPS), Internet Protocol (IP) address or Media access control (MAC) address from the user's phone. Location authentication refers to use of location data to access/deny entry into a system. Geolocation based authentication scheme ensures security of mobile transactions based on the user location (Akoramurthy & Arthi 2017).

The need to secure private or sensitive information in mobile devices is one of the main problems in information security. Today smartphones are a central place to a great deal of users' private information and are thus a primary target for cyber-attack, with the main goal of the attacker being try to access and exfiltrate the private information stored in the smartphone without detection (Yisroel *et al.* 2017). Traditional authentication mechanisms like PINs, patterns and passwords being the most widely used authentication techniques suffer from well-known limitations and drawbacks in the security community such as shoulder surfing, key logging, brute force, guessing attack and phishing attacks (Alzubaidi & Kalita 2016), Weizhi *et al.* (2018). As a response to such incidents security researchers have started to investigate other alternative authentication methods.

Currently there is a growing body of research to improve user authentication based on physiological and behavioral biometrics (Habib & Alqatawna 2017). Keystroke dynamics behavioral biometrics falls under behavioral biometrics and (IBIA 2017) described it as the future of user authentication. The essential reason of keystroke dynamics authentication is that everybody is unique whereas the use of location verification takes advantage of personal information, assuming that such information are easily remembered by users and at the same time hard to guess by others Hang *et al.* (2015) forming the basis of our proposed authentication. Mobile banking is becoming one of the essential feature that is demanded by almost every smartphone user and it is with this reason that banks are reaching out to its users (Akoramurthy & Arthi 2017) via mobile platforms. Successful implementation of Mobile banking largely depends on the extent of how much customers are fully motivated to adopt it with trust in the bank service being among the key issues (Ali *et al.* 2017).

The implication and contribution of this paper sought to build upon on the knowledge of mobile banking security as it proposes use of keystroke dynamic and location verification authentication as an alternative method of securing mobile transactions. This paper includes the authentication based on user's behavior and location data that consist of PIN typing and location time stamps.

The rest of this paper is structured as follows: Section 2 presents related work covering what other researchers had done in authentication highlighting the different authentication types and later on an evaluation of the existing authentication methods are presented. Section 3 gives an explanation of the proposed authentication method and the experimental set up. Section 4 describes the results and discussion of the experiments. Section 5 gives a conclusion of the paper and the suggested future research work.

2. Related Work

Patil & Renke (2016) found out that the idea behind keystroke dynamics authentication appeared in the twentieth century when telegraph operators could authenticate each other based on their distinctive patterns when keying messages on telegraph lines. Another study by Ho & Kang (2015) reported that Keystroke dynamics based authentication was one of the prevention mechanisms used to protect one's account from criminals' illegal access. In this authentication mechanism, keystroke dynamics are used to capture patterns in a user typing behavior. In their findings Pahuja & Nagabhushan (2015) revealed that usernames could be easily known and passwords could be easily guessed. As the passwords are simple, they are vulnerable to attacks like phishing attacks and brute force attacks etc. They suggested that a better way to strengthen the PINs and passwords was to combine them with biometrics which comprises of behavioral or psychological biometrics.Babaeizadeh *et al.* (2014) proposed the use of Keystroke Dynamic in providing security for Mobile Cloud Computing (MCC) with an aim to verify user's identity when they wish to request services via the Internet through Cloud Service Provider (CSP).They found out that through use of keystrokes it became very difficult for an attacker to pretend as the owner. The results of their experiments showed, that their proposed method could work 97.014% correctly, due to the keystroke duration of each user depending on their behavioral characteristic and it can be measured up to milliseconds.

(Hyungu *et al.* 2018) reported that by combining PIN (or pattern) and keystroke dynamics as a multifactor authentication, keystroke dynamics strengthens user authentication. Keystroke Dynamics is a two factor biometric security. For a successful login into the system, firstly password should be known and secondly, typing pattern should match Vinayak & Komal (2015). When it comes to location verification a study by (Hang *et al.* 2015) found out that users were good in recalling the location-answers to their questions while strangers failed most of the time when attacking these questions.

The use of mobile devices with GPS facility is increasing in daily life. GPS sensors are nowadays present in 85% of mobile devices, which means that it is now common for apps to access a user's geographical position (Kiefer *et al.* 2018). The GPS receiver that is inbuilt in smartphones captures the real location with its attribute like latitude, longitude of the user giving the location information that gets stored in the server's database along with the time stamp those changes readily time to time. GPS is a space-based satellite navigation system that provides location and time information in an all-weather conditions, anywhere on or near to the Earth where there is unobstructed line of sight to four or more GPS satellites, Fridman *et al.* (2017) found that there were two key characteristics of the GPS location data. One, it was relatively unique for each individual even for people living in the same area of a city and two, outside of occasional travel, it does not vary significantly from day to day and with this captured with the help of google maps.

Research from Juniper Research (2016) reported that over 2 billion mobile users will have used their devices for banking purposes by the end of 2021, compared to 1.2billion as at 2016 globally. Growth in mobile banking is being driven by consumer adoption of banking applications changing way consumers manage their finances. While consumers continue to express concern over using their mobile phone to conduct banking and financial services transactions, it is a fear born more of perception than reality. There are threats, but the security controls available to mitigate risk at this level are substantial and effective. However, security practices will need to continue to evolve as more and more smart phones enter the market running more and more applications, creating an ever growing opportunity for security threats (Md. Shoriful 2014).This paper aims to improve on the weakness of PINs authentication by incorporating keystroke dynamics into PINs and location data which are unique to a user. The presented approach in this paper uses the typing behavior also known as keystroke of a user to create a profile for the user and the validity of location visited by the user.

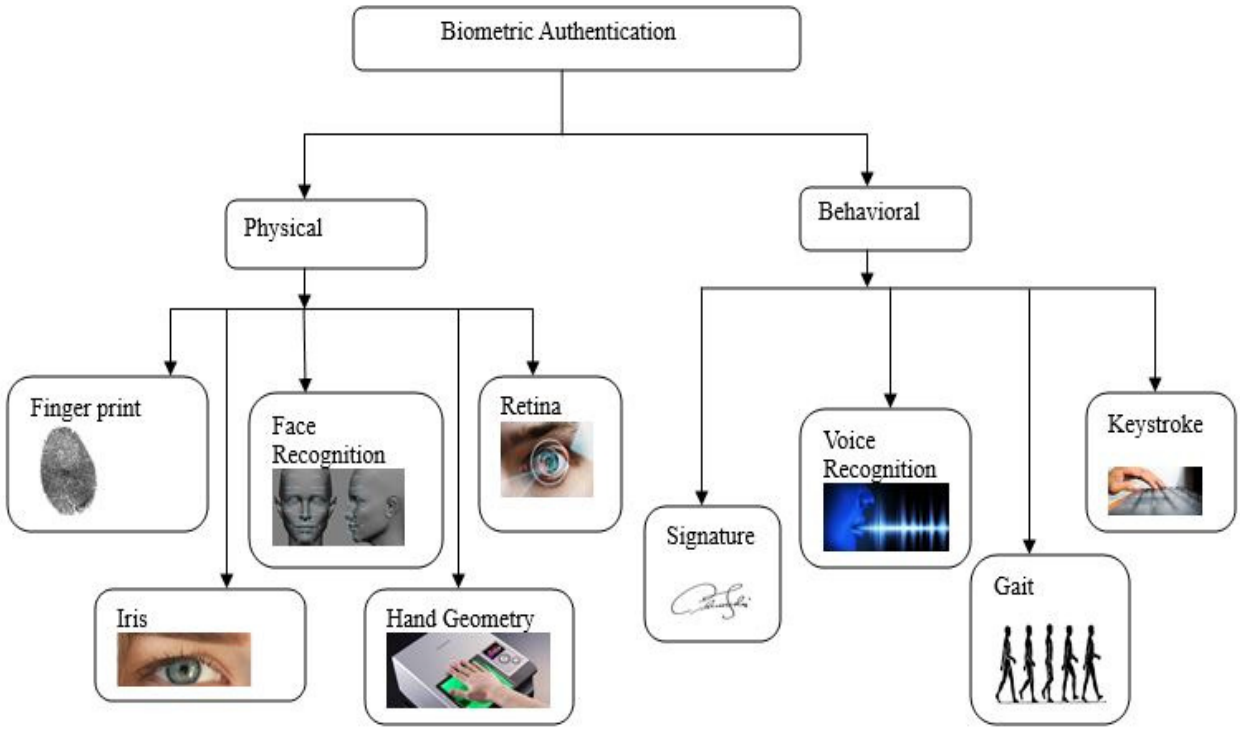

Figure 1. Biometric Authentication Types (Mahnoush *et al.* 2014).

Table 1. Authentication Evaluation Table

Authentication Method	Features	Improvement	Limitation
1. Personal Identification Number (Weizhi *et al*. (2018)	• 4-8 digits	• Preventing unauthorized person accessing a mobile phone. • It's limited to number of trials e.g 3 times	• Easy to guess PINS
2. Password Authentication (Nosrati & Massoud 2016)	• Can contain a string of letters, special characters and numbers.	• Provides a large number of set of passwords in comparison to PIN length of a password is dependent on the security policy of the particular application.	• Difficult to type long password on small keypads. • Use of default passwords that make it easy to login.
3. Recognition-based passwords Authentication (Sudeep & Reshma 2017)	• Pattern length 4-9		• This technique provides less number of password patterns than traditional PIN and password.
4. Token based authentication Nosrati & Massoud (2016)	• fast authentication	• Requiring minimal user interaction compared to other authentication techniques. • Increase user convenience over the secret-knowledge approach.	• Tokens cannot be replaced as easily as passwords.
5. Transparent authentication (Maria *et al.*2015) (Mohammad & Sheikh 2014) (Maghsoudi & Tappert 2016)	use of • Keystroke dynamics • Gait (walking sensors) • Signature • Mouse • Iris • Face • Finger print • Palm print	• Identity uniqueness of each user • No need to cram or remember authentication is based on what the user has	• Some require considerable computing power. • Takes more time for authentication and requires high-cost additional hardware.

3. Experimental Set Up

To able to capture user's keystroke behavior this study used a touch screen keyboard sensors available on

android operating systems which is an open source software that most smartphones operate on, through a prototype of a mobile banking application that stores the typing data as users keyed in their PINs. The location data was obtained through the phone's cellular data, Wireless networks or GPS.Training and testing of the system was done to learn user's typing patterns through classification which is used to differentiate legitimate user's profile from an imposter as user's key in their PINs by recognition and reference based on stored data in the database.

3.1 Keystroke Capture

Through use of in built touch screen keyboard sensors available on smartphones user's typing behavior is captured which later on used to characterize the user's unique typing behavior. This takes place as users' type in their 4 digit PINs during registration of new users and authentication of registered users. Keystroke capture stores the timing information in relation to the pressed key buttons.

3.1.1 Location Capture

In the background as the user types their PIN, their location is captured via a GPS module which determines the device's location under any weather condition at any time from a smartphone, Location information can also be obtained through a smartphone' cellular data and through access of Wireless networks.

Location Based Authentication Algorithm Mathematical Module *(*Chitra *et al.* 2015)

1. User (U) this is actor handles system functionality.
SET OF U= {1.....N}

2. Capture GPS Co-ordinates of User Device Latitude and Longitude factor.
2.1 Get Stored Location Co-ordinates Latitude and Longitude factor.
2.2 Calculate Distance between capture Co-ordinates and Stored Co-ordinates to define the periphery i.e. certain range within which user can get access to the data.

Formula-

Var phi1=lat1 to radian ( )
Var phi2= lat2 to radian ( )
Δlambda= (long2-long1) to radian ( )
Doubledist=Math.sin(phi1)*Math.sin(phi2)+Math.cos(phi2)
Math.cos(Δlambda);
Output = Find Nearest Location.

3.1.2 Training Phase

When the users will be typing their PIN for the first time the system will prompt them to type their preferred PIN 10 times. As a background process this trains the system for recognizing user's typing behavior which will be used to recognize the user the next time they access the system It is in this phase that the user's unique profile is generated based on their uniqueness in typing following successful training.

3.1.3 Recognition and Reference

Following the stored user's profile in the database each time the user types in their PIN, a comparison based on the stored profile is done. Upon successful recognition in obtaining a user's behavioral profile the user will be prompted to verify their transaction location this is done verify in reference to the captured location that this is the actual user trying to gain access to the application.

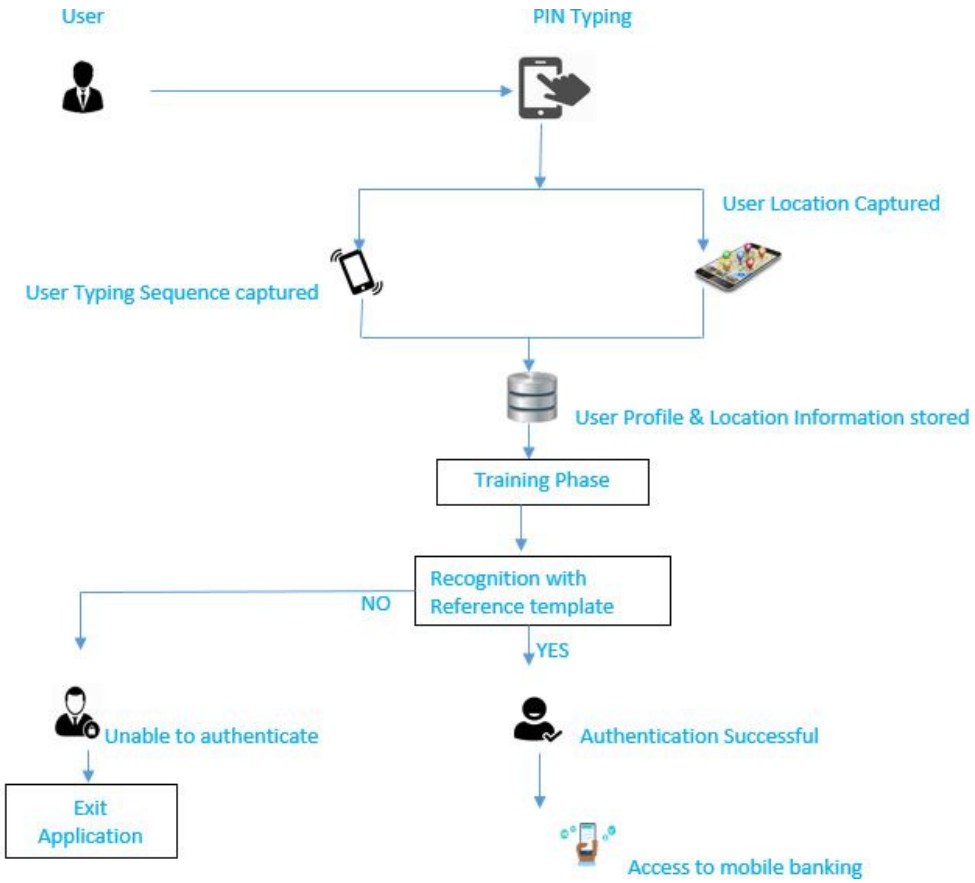

Figure 2. Proposed Authentication Method

3.2 Composition of the proposed authentication method

The proposed alternative method for securing mobile transactions is based on keystroke dynamics which is an improvement from the study of Singh *et al.* (2017) on behavioral profiling users as they type their passwords having features such as keyboard monitoring, features extraction, classifier algorithm and a database. In their study they reported that keystroke dynamics was not enough by itself which is why this study seeks to improve the authentication method with the addition of location verification which ensures security of mobile transactions based on the user's transaction location captured by smartphones GPS sensor and it' application to mobile banking.

3.3 Keystroke Dynamics

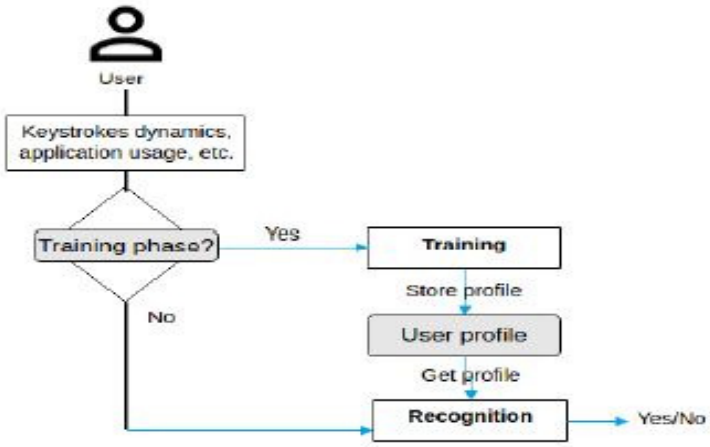

Figure 3. Singh et al. (2017) User Profiling

3.4 Location Verification

Based upon the hypothesis that people have a predictable travelling pattern, a user's location can be detected through use of mobile cellular network or through Global Positioning System (GPS) link (i.e. longitude, latitude).The utilization of location in an application could contribute information towards to successful identification of a user Li *et al.* (2014).By recording the users' location information over a time period and combining the location information pattern with the keystroke profile creates a distinctive verification to a user which is unique to each individual. Knowing where an application was used, majority of the users can be differentiated. This methods can provide sufficient discriminatory information to identify mobile users. A study by Kuseler & Lami (2012) showed concern of getting user's geographical location as an important authentication factor to enhance security of mobile commerce applications, especially those requiring robust client authentication.

3.5 Experiment

Two experiments were conducted comprising of Kenya Commercial Bank (KCB) head office branch staffs. The respondents had advanced level of skill when it came to smartphone use and experience with mobile banking. From the survey out of the sampled 138 respondents, 60 respondents indicated to have an advanced level of skill. KCB is the largest bank in Kenya accounting for 13% of all assets (global credit rating 2013) .The reason for choosing KCB was because its mobile banking service was declared the best in Kenya (Thinking Business Awards 2017). Users of KCB mobile banking application are able to pay key monthly bills such as electricity (both postpaid and prepaid account holders), DSTV and Zuku, payment of merchants can also be paid directly via the App.The sampled respondents had advanced level of skills when it came to smartphone use and experience with mobile banking based on the survey findings and their participation in this experiment was ideal for evaluating the proposed alternative authentication method.

3.5.1 Validation of the proposed authentication method

Method validation defines an analytical requirement and confirms that the method which is under consideration has the performance capabilities that are consistent with what the application requires. The proposed authentication method was subjected to tests both with legitimate users and 10 imposters who were selected at random and issued with users account and PIN numbers to try and access their accounts within 5 attempts over a period of 30 days. Results were measured in percentages using biometric metrics of FRR, FAR and ERR over a period of 30 days later on the results were compared with the findings of other researchers. (Alotaibi *et al.* 2015) in their study found out that the performance of a typical biometrics technique is measured by False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). FAR refers to the percentage of access attempts by imposters that have been accepted by the system (incorrectly accepted) whereas FRR refers to the percentage of access attempts by legitimate users that have been rejected by the system (incorrectly rejected). In this context, low FAR indicates that the system is secure, and low FRR means the system is usable. The point at which FAR and FRR are equal is called EER, which means that a system is accurate. To be a more accurate and better performing system, the system needs a low EER

False Rejection Rate (FRR) calculated using the following expression

$$FRR = \frac{\text{Number of genuine rejections}}{\text{Number of genuine attempts}}$$

False Acceptance Rate (FAR) calculated using the following expression.

$$FAR = \frac{\text{Number of unauthorized accepts}}{\text{Number of unauthorized attempts}}$$

3.5.2 Experiment 1: Use of PIN authentication

Here a mobile banking application that required use of account number and PIN number for authentication was used among the selected participants. In this experiment the objective was to subject users on use of traditional authentication methods such as PINs and Passwords and what their preferences were when it came to creating them and whether the default settings issued by the bank were changed and examine their considerations for authentication.

3.5.3 Experiment 2: Use of Keystroke dynamics and Location verification

In the second experiment a mobile banking application that used PIN incorporated with use of Keystrokes and location verification was used as part of user authentication. Users were required to type their PINs 10 times as the system trained on identifying user's unique typing behavior each time typed. Location data was captured through the phone's GPS, Wi-Fi or Cellular data as the users interacted with the application in making transactions such as payments for their bills, cash deposits and withdrawals among others. The obtained data was used to create user's profile. Later on determination on the uniqueness of each user in terms of profiling and the location of the transaction was carried out.

4. Results and Discussion

4.1 Experiment 1: Use of PIN authentication

The experiment sought to find out how often or rarely the users changed their PINs and if they carried out most of their transactions at different locations. This was carried out within a period off 30days on the sampled population. The objective in this experiment was to demonstrate that PIN only authentication could not distinguish a legitimate user from an unauthorized user as when both were issued with an account number and PIN they could access the account easily.

Table 2. Authentication Complexity

Regular change of PINs	
Change of Registered PIN	25%
No change of PIN	75%

4.2 Experiment 2: Use of Keystroke dynamics and Location verification

This experiment incorporated use of Keystrokes and location verification as part of user authentication on the mobile banking application. For a period of 30days users were subjected this method of authentication. A prototype of a mobile banking application that operated on android and was used. This application provided services that users were able to carry out transactions such as payments for their bills, cash deposits and withdrawals among others. When users registered on the application personal information such as their names, mobile number, identification number were collected after which they were prompted to type in their PINs 10 times after which the application created their keystroke profile based on timing information from their typing behavior and also their current location. Every time the user accessed their account the application sought to compare the stored profile together with the indicated transaction location and when a match was found the user was allowed access. The objective here was to demonstrate how the system could be able to distinguish a legitimate user from an imposter based on the uniqueness of the user's typing behavior and their transaction location.

Table 3. Unique keystrokes and location across different users

User ID	Typing Sequence Speed	Category of Transaction Location
1	**2000**	**Home**
13	**4000**	**Work**
12	**7000**	**Work**
20	**3000**	**Home**
33	**5000**	**work**
37	**15000**	**Entertainment spot**
40	**6000**	**shopping**
47	**9000**	**work**
55	**12000**	**work**
60	**10000**	**home**

Table 4. Sample user Training Results

Registered User	**PIN Used**	**PIN Typing attempts**
1	0004	10
2	4321	10
12	7777	10
20	2015	10
33	8124	10
37	0938	10
40	2018	10
47	3533	10
55	1234	10
60	4433	10

Table 5 Sample user Testing Results

Registered user	PIN		Expectation	Actual Result
1	0004		Authenticate	Authenticated
2	4321		Authenticate	Authenticated
12	7777		Authenticate	Authenticated
20	2015		Authenticate	Authenticated
27	2471		Authenticate	Authenticated
21	1988		Authenticate	Authenticated
24	1992		Authenticate	Denied
33	8124		Authenticate	Authenticated
42	2018		Authenticate	Authenticated
47	3533		Authenticate	Denied
55	1234		Authenticate	Authenticated
Non Registered User No.	Name	PIN Used	Denied	Denied
3	Patrick	8124	Denied	Denied
4	Timothy	3533	Denied	Denied
7	Mary	0004	Denied	Authenticated
9	Jane	2018	Denied	Denied
10	Timmy	4321	Denied	Denied

Table 6. Use of keystroke dynamics and location verification

The use of proposed authentication method on mobile banking		
Statement	Frequency	Percent %
Strongly agree	28	47%
Agree	13	22%
Neutral	12	20%
Strongly disagree	2	3%
Disagree	5	8%
Total	60	100%

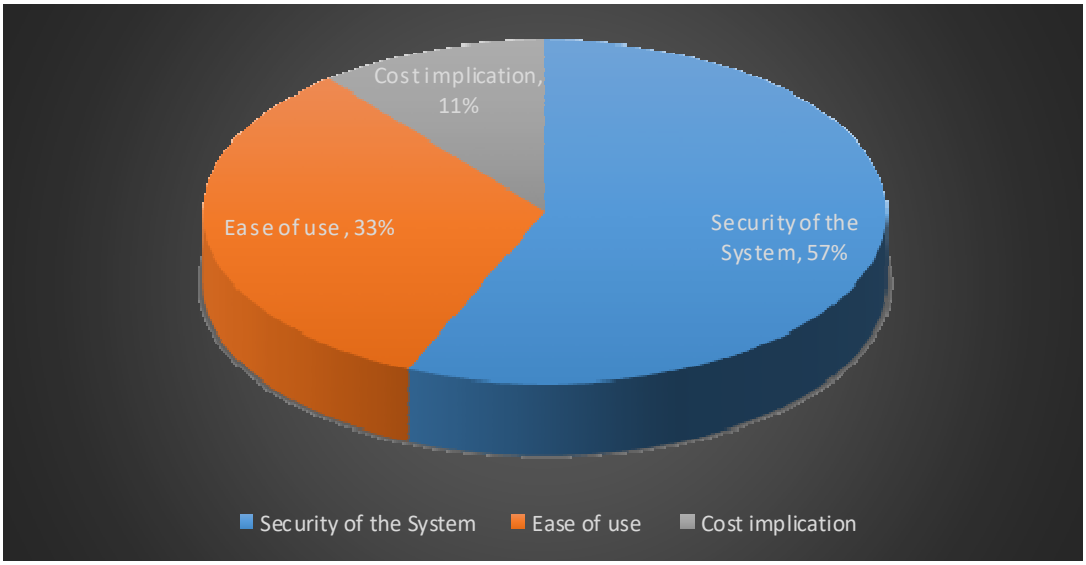

Figure 4. Concern in using the proposed authentication method

4.3 Discussion of Results

From the first experiment carried out users usually tend to use easy PINs that could easily be bypassed when they were the only form of authentication as the user's account can be accessed by an intruder. User formulated their PINs around current year, their date of birth and similar sequence of digits that they found easier to remember. Similar to the findings of this paper a study by the (Data Genetics 2012) found the second most popular PIN was 1111, followed by 0000, 1212 and 7777.They reported that Many people also used the year of

their birth to create their PIN, with every single combination of the digits in the years 1901 to 1999. When compared with the second experiment with incorporation of keystroke dynamics and location verification where the respondents still used the same PINs, it was challenging from the randomly selected people who acted as imposters to intrude the application even when the users PIN were shared to them.

As much as the intruder had the user's PIN they could not match the stored user's profile which was unique to each user. A study by Singh *et al.* (2017) shared similar findings where they found that in that Keystrokes dynamics are a part of behavioral biometrics and are unique to a person. Another study by Mahfouz *et al.* (2017) on behavioral biometric authentication on smartphones found that due to the weaknesses of the traditional authentication mechanisms such as PIN, Pattern and Password, the research community proposed the development of authentication mechanisms based on behavioral biometric traits such as gesture, keystroke and gait. These mechanisms are known as active or continuous authentication mechanisms.

Majority of the respondents interacted more with the application that incorporated use of behavioral profiling and location verification in mobile banking applications where they performed more transactions compared to the earlier one that had Pin only authentication. Similar to this findings was a study by Ciampa *et al.* (2013) where they found that users were willing to deal with more than the usual user name/password authentication if it meant stronger security. Another comparison that shared with this findings was a study by Butler & Butler (2015) reported that users had a high degree of acceptance of 'risk-based' authentication, in which a positive inclination was towards the user's identity based on such things as log-on location, IP address, and transaction behavior.

From the experiments 60 legitimate users' samples were collected over a trial period of 30 days with 10 attempts of logging into the system and 10 random people who were randomly selected to be imposters with each having 5 attempts over the 30days period. Comprising of 60 genuine users a total of genuine attempts made were 300 while the number of unauthorized attempts made were 3000.The results gave a False Rejection Rate (FRR) of 5.33% which is the percentage of access attempts by legitimate users that have been rejected by the system and a False Acceptance Rate (FAR) of 3.3% which is the percentage of access attempts by imposters that have been accepted by the system incorrectly, giving an Equal Error Rate (EER) of 4.3%.Li *et al.* (2011) study found that on the application level profiling of a user activity experiment they got an EER of 13.5% which compared to the results of this study saw is an improvement having an EER of 4.33% .The False Acceptance Rate 3.3% and False Rejection Rate 5.33% results of this paper found to be lower compared to the findings of (Noor & Mudhafar 2016) that reported a false acceptance rate at 5% false rejection rate is 5.6%.

Elsewhere a study by Kambourakis *et al.* (2014) on Keystroke Authentication System for smartphones concluded that Keystroke authentication which is an authentication based on how a user types had significant potential in designing enhanced authentication systems destined to future smartphones after they obtained an a minimum EER value of 12.5%. The proposed authentication method has little costs implications to the current smartphones that operate on android system and works in the background causing no interruptions as one uses the application and offers an alternative security method which were concerns raised by the respondents. This findings are similar to the study of Ciampa *et al.* (2013) where they found that 'consumers are willing to take extra steps to protect their identities, but they do not necessarily want to pay extra for these services.

The experiments carried out shows that mobile banking users use easy PINs which can be costly to the bank customers and banks in general. The Kenya Cyber Report (2015) reported that the individuals who have subscribed to mobile banking services risk exposure to cyber related criminal activities and found a gap in security controls put in place for mobile money services. It is for this reason that this research aims to address this gap by proposing an alternative authentication method which is use of keystroke dynamics and location verification. From the results of the experiment the evaluation of the proposed authentication method showed it was offering an alternative method of securing mobile transactions as it provided improvement compared to previous studies.

5. Conclusion and Future Work

This paper sought to evaluate existing authentication methods in mobile banking together with their threats and vulnerabilities and to propose use of Keystroke dynamics and location verification as an alternative method of authentication in mobile banking. This paper addressed the weaknesses of PIN only authentication by proposing a method that uniquely identifies a user's typing behavior and the location of the transaction to be able to access their accounts. The proposed method added a distinctive feature that even though users used weak PINs an unauthorized users could not be able to access their account as it was difficult to type as a legit user and be at the same location with them. The findings of this research showed an improvement from previous studies having shown better results.

The proposed authentication method aims improve on the use of PINs and Passwords only authentication incorporating users behavior that uniquely identifies each user, having obtained a FRR of 5.33% and FAR of 3.3% where if the FAR is low and the FRR is high it would ensure an unauthorized person would not be allowed

access and that at times authorized people would need to type in their PINs several times before they are allowed access. Security remains a major concern on any system and for banks to be able to counter cyber related activities banks will be required to stay up to date by addressing security control gaps emerging with the technological advancements in the mobile banking services. In this paper the use of keystroke dynamics and location verification was proposed as an alternative authentication to mobile banking, future work would focus on its implementation in the Automated Teller Machines (ATM) lobby. Further research would be on how to integrate user typing behavior and location verification to bank Automated Teller Machines (ATMs).

References

Akoramurthy, B. & Arthi, J., 2017. *GeoMoB — A geo location based browser for secured mobile banking,.* Chennai, doi: 10.1109/ICoAC.2017.7951750, pp. pp. 83-88.

Alariki, A. A. & Manaf, A. A., 2014. *Biometrics Authentication Using Touch-Based Gesture Features for Intelligent Mobile Devices.* Johor, Malaysia, s.n., pp. 528-538.

Ali, A. A., Yogesh, K. D. & Nripendra, P. R., 2017. Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management,* pp. vol 37.PP 99-110.

Alotaibi, S. n., Furnell, S. & Clarke, N., 2015. *Transparent authentication systems for mobile device security: A review.* s.l., DOI: 10.1109/ICITST.2015.7412131, pp. 406-413.

Anon.,2012.*DataGenetics.*[Online] Available at: http://www.datagenetics.com/blog/september32012/.

Asif , A., Israr , u. H. & Monisa, . N., 2017. Two Factor Authentication. *International Journal of Computer Science and Mobile Computing.*

Babaeizadeh, M., Bakhtiari, M. & Maarof, M. A., 2014. Authentication Method through Keystrokes Measurement of Mobile users in Cloud Environment. *Int. J. Advance Soft Compu. Appl,* pp. vol. 6, no. 3.

Butler, M. & Butler, R., 2015. *Investigating the possibility to use differentiated authentication based on risk profiling to secure online banking.* s.l., https://doi.org/10.1108/ICS-11-2014-0074, pp. Vol. 23 Issue: 4, pp.421-434.

Chang, T., 2012. Dynamically generate a long-lived private key based on password keystroke features and neural network. *Information Sciences,* pp. 36-47.

Ciampa, M., Enamait, J. & Mark, R., 2013. A Comparison of User Preferences for Browser Password Managers. *Journal of Applied Security Research,* pp. Vol. 8, No. 4,pp455-466.

Ehatishamulhaq, et al., 2017. Authentication of smartphone users based on activity recognition and mobile sensing.. *Sensors,* p. 17.

Fenu, G. & Pau, P. L., 2015. *Modeling user interactions for conversion rate prediction in M-Commerce.* Larnaca, doi: 10.1109/ISCC.2015.7405533, pp. 309-314.

Fridman, L., Weber, S., Greenstadt, R. & Kam, M., 2017. Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. *IEEE Systems Journal,* pp. vol. 11, no. 2,513-521.

Gundecha , S. S. & Naidu, M., 2016. Multilevel biometric authentication by using different techniques. *IEEE International Conference on Advances in Electronics,Communication and Computer Technology,* pp. 50-54.

Habib, M. & Alqatawna, J., 2017. *A Proposed Password-Free Authentication Scheme Based on a Hybrid Vein-Keystroke Approach.* Amman, doi: 10.1109/ICTCS.2017.27, pp. 173-178.

Hang, A. et al., 2015. *Where have you been? Using location-based security questions for fallback authentication.* s.l., s.n., pp. 169-183.

Heikkilä, J., Li, H. & Liu, Y., 2014. Understanding the factors driving NFC-enabled mobile payment adoption. *An empirical investigation,* p. 231.

Ho, J. & Kang, D. -K., 2015. Sequence alignment with dynamic divisor generation for keystroke dynamics based user authentication. *Journal of Sensors.*

Hyungu, L. et al., 2018. Understanding Keystroke Dynamics for Smartphone UsersAuthentication and Keystroke Dynamics on Smartphones Built-In Motion Sensors. *Security and Communication Networks,* p. Volume 2018.

IBIA,2017.[Online]Availableat:https://www.ibia.org/biometrics-and-identity/biometric technologies/behavioral-biometrics.

Ivannikova, E., David, G. & Hamalainen, T., 2017. *Anomaly detection approach to keystroke dynamics based user authentication.* Heraklion, Greece,, doi:10.1109/ISCC.2017.8024638, pp. 885-889.

Jeong, B. K. & Yoon, T., 2013. An Empirical Investigation on Consumer Acceptance of Mobile Banking Services. *Business and Management Research,* pp. vol. 2, no. 1, 31-40.

Juniper, R., 2016. *Retail Banking: Digital Transformation & Disruptor Opportunities 2016-2021,* s.l.: Retrieved from https://www.juniperresearch.com/researchstore/fintech-payments/retail-banking.

Kambourakis, G., Damopoulos, D., Papamartzivanos, D. & Pavlidakis, E., 2014. Introducing touchstroke:

Keystroke-based authentication system for smartphones. *Secur. Commun. Netw,* pp. pp. 1-13.

Kang, P. & Cho, S., 2015. Keystroke dynamics-based user authentication using long and free text strings from various input devices. *Inf. Sci.,* pp. vol. 308, pp. 72-93.

Kiefer, P. et al., 2018. *Detecting Location-Based User Actions.* s.l., ETH Zurich.

Kigen, P. M. et al., 2015. *Kenya cyber security report,* Nairobi: http://erepo.usiu.ac.ke/bitstream/handle/11732/1466/KenyaCyberSecurityReport2015.pdf?sequence=4.

Koong, C. S., Yang, T. -I. & Tseng, C. -C., 2014. A user authentication scheme using physiological and behavioral biometrics for multi-touch devices. *The Scientic World Journal.*

Kuseler & Lami , 2012. Using Geographical Location as an Authentication Factor to Enhance mCommerce on Smart Phones. *International Journal of Computer Science and Security,* pp. 277-287.

Maghsoudi, J. & Tappert, C., 2016. *A Behavioral Biometrics User Authentication Study Using Motion Data from Android Smartphones.* s.l., s.n.

Mahfouza, A., Mahmouda, T. M. & Eldinc, A. S., 2017. A survey on behavioral biometric authentication on smartphones. *J.Inf. Security Appl.,* pp. 28-37.

Mahnoush, B., Majid, B. & Mohd, A. M., 2014. Keystroke Dynamic Authentication in Mobile Cloud Computing.. *International Journal of Computer Applications ,* pp. 29-35.

Manal , A. & Haydar, T., 2016. *Network Security Threats and Vulnerabilities.* s.l., s.n., pp. 115-121.

Maria, D. M., Michele, N., Daniel, R. & Harry, W., 2015. Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols. *Pattern Recognition Letters,* pp. 17-23.

Mohammad, T. & Sheikh, I. A., 2014. *Your Phone Knows You: Almost Transparent Authentication for Smartphones.* s.l., doi>10.1109/COMPSAC.2014.60, pp. 374-383.

Mouna, J., Latifa, B. A. R. & Anis, B. A., 2014. *Classification of security threats in information systems.* s.l., In ANT/SEIT.

Noor, M. A.-O. & Mudhafar, M. A.-J., 2016. *Statistical Keystroke Dynamics System on Mobile Devices for Experimental Data Collection and User Authentication.* Liverpool, doi: 10.1109/DeSE.2016.21, pp. 123-129.

Pahuja, G. & Nagabhushan, T. N., 2015. *Biometric authentication & identification through behavioral biometrics: A survey,.* Noida, doi: 10.1109/CCIP.2015.7100681, pp. pp. 1-7.

Pisani, P. H. & Lorena, A. C., 2013. A systematic review on keystroke dynamics. *Journal of the Brazilian Computer Society,* pp. vol.19,573-587 .

Purgason, B. & Hibler, D., 2012. security through Behavioural Biometrics and Artificial Intelligence. *Procedia Computer Science,* pp. vol 12, 398-403.

Rohit, A. P. & Amar, L. R., June,2016. Keystroke Dynamics for User Authentication and Identification by using Typing Rhythm. *International Journal of Computer Applications,* pp. volume 144, No.9,(0975 –8887).

Shih, D., Lu, C. & Shih, M., 2015. A flick biometric authentication mechanism on mobile devices. *International Conference on Informative and Cybernetics for Computational Social Systems,* pp. 31-33.

Shivhare, B., Sharma, G., Kushwah, R. S. & Kushwah, S. P., 2015. *Using Geo-location method for lost node in location based services.* Gwalior, doi: 10.1109/ICCN.2015.68, pp. 356-360.

Shoriful, I., 2014. Systematic Literature Review: Security Challenges of Mobile Banking and Payments System.. *International Journal of u-and e-Service, Science and Technology,* pp. 7:107-116.

Shoriful, M. I., 2014. Systematic Literature Review: Security Challenges of Mobile Banking and Payments System. *International Journal of u-and e-Service Science and Technology,* pp. vol. 7, pp. 107-116.

Singh, D., Bhawnesh, J., Himanshu, N. & Amit, K., 2017. Presskey- A Keystrokes Dynamics Based Authentication System. *International Journal of Advanced Research in Computer Science,* p. vol.8 no.5.

S, S. M. et al., 2015. Three Factor Authentication using Location. *International Journal of Engineering and Innovative Technology (IJEIT),* pp. Volume 4, Issue 7,.

ThinkingBusinessAwards,2017.[Online]Availableat:https://www.businessdailyafrica.com/corporate/companies/KCB-named-Bank-of-Year-at-global-fete/4003102-4216150-10s4bj8z/index.html.

Vinayak, R. & Arora, K., 2015. A Survey of User Authentication using Keystroke Dynamics. *International Journal of Scientific Research Engineering & Technology,* p. Volume 4.

Weizhi, M. et al., 2018. TouchWB: Touch behavioral user authentication based on web browsing on smartphones. *Journal of Network and Computer Applications,* pp. 1-9.

Wu, F., Xu, L., Kumari, S. & Li, X., 2015. A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks. *Comput Electr Eng,* p. 274–285.

Yisroel, M. et al., 2017. Anomaly detection for smartphone data streams. *Pervasive and Mobile Computing,* pp. vol. 35,83-107.