Music Wave Token Password for Mobile Phone

Oyinloye Oghenerukevwe E, Ojedayo Benson O., Akinbohun Folake O.

Abstract—Mobile devices security has been a major challenge mostly because the operating system are seldom expected to include restrained observed vulnerabilities and generally is not as secured as develop computers. Although this has not stopped usage by it is customer method PIN, password, patterns or available biometric options have been used most of which are seen to be inconvenient or uninteresting for users. This paper present on improvised music token for password operation deployable on a mobile phone. Using the piano key of two white and two black keys with a large keypool to profer acceptable security system.
The system has two stages, a protection and verification stage which is secured based on matrix calculation. The system was tested be resistant to dictionary, shoulder surfing and general attacks as the frequency of keystrokes is key to tune generation.

Index Terms— Frequency, Music, Token, keypool, Matrix, Tune, beat Segmentation, chroma, authentication, verification.

1 Introduction

Mobile phones have become part of our lives aiding our works and access to user determined special data. These devices are relatively small and economical they can be used for voice calls SMS, emailing access to internet resources and many more function, which were once limited to desktops and laptop computers. These mobile phones are even used for entertainment and e-commerce activities. With over 100 million smartphones in the hands of people, it has become the most influential technology and business driver in the world today.
These mobile phones are designed to make installation and use of third party applications possible aiding increased in vast usages. This advantage has opened up a high risk of security breaches for users posed by attackers. This risk is seen major on mobile device platforms that do not place secondary restrictions on third party application, further; these third party applications due to the poor security measures as well as lack of update on most mobile phone operating system may inject malware into the devices that perform great havoc need to provide/use multiple security options thereby ensuring confidentiality, integrity and availability. Although currently mobile phone designers have provided low acces control devices called locked and unlocked [1] Most smartphones offer optional locking mechanism which majorly protect the user from physical intruders not internet or network intruder, although this paper will concentrated on providing protection from physical intruders but an enormous work needs to be done on protection from internet / network intenders.
Locking mechanisms such as personal identification number (PIN) password, pattern, biometric featured authentication have been proposed and used to restrict physical access to the devices [2][3].
All these are essential to protect the devices from physical theft as they provide data protection [11]
While physical data protection is essential another critical need is the protection form hackers, hackers may use mobile devices as an access point into many other aspects of daily digital life as well as the lives of others within a user's network, making mobile security a costly fit. Government organizations are attempting to reduce this said problems by setting standards, laws and forcing agencies to comply with these standards.
Most systems today depends on static passwords (static in the sense that most systems can use the same password combination for long time without requesting change) to authenticate users identity. However these password come with the major management of security concerns that have been exploited by attackers which is been in dictionary attacks [2], other problems with these passwords include easy to guess, use of the same password is numerous account, writing and storage of password to avoid forgetting (especially for string passwords).
Other attacks on password include shoulder surfing, snifing, keyboard stroke guessing [2] Several strategies which include fingerprint, facial, pattern have been suggested and use, most of which are not convenient for users
The not convenient issue of the mentioned security measures, used in phones is seen in the report of [13] who worked on voice recognition as an authentication, stating that a person's voice print can be unique as any other biometric characteris-

- *Oyinloye Oghenerukevwe E, Ojedayo Benson O., are staff of Ekiti State University, Computer Science and Computer Engineering respectively . E-mail: rukkivie@yahoo.com; bojedayo@gmail.com*
- *Akinbohun Folake O. is a staff of Rufus Giwa Polytechnic,Owo, Ondo State Nigeria)*

2 Literature Review

To proffer security solutions to mobile phones there may be a

tics as long as the correct analytical technologies are used and this feature based the report says may be detrimental on a false acceptance as a possible facing of one's voice leaves the system vulnerable; observation shows that the human voice can be mix matched and mostly not differentiable from the original users or voice owner making the approach vulnerable to voice recomptation attacks.

Finger print recognition which is based on exploiting the unique nature of the human finger print is also another type of security authentication which is said to be safe [7] but firstly most mobile devices used do not carry this features hence many be said not be readily available for use by all mobile phone users furthermore the mobile phone user can be social enquired to authenticate his/her mobile device [12]. In a case of destruction of finger print pattern for example in a fire accident the print will be distorted and the user can no longer authenticate his/her device.

For face defection based system, light contrast is one of the major problems; a poorly lighted environment will mean not been able to detect the face thereby giving a false rejection report. Although with facial authentication it is almost impossible to hack into the system it is user friendly, a lot more appreciated easier to use than remembering password it is cheap as most devices come with a camera and requires no extra cost to implement it [10].

Personal identification numbers pin are also available, pin generally consist of 0-9 digits or mostly four to eight combination required. The more pin combination required the less interrelated effort in used to remember the pin [2].

The iris is another mode of authentication on mobile phones the unique pattern in an iris is detected and the used as authentication [8] with high quality image or a convincing reproduction of an eyeball the iris scanner can be successfully attacked [8] even though the cameral calculates the pattern in an eye iris.

Music is seen as a primary inspiration that leads to greater memorization and decrease the tendering to choose insecure password. It has been observed that a human's ability to remember music is much more powerful that the ability to remember texts [4][5].

[6] Work on musical passwords and found out that any musical device can be used to enter musical password. He used a piano to generate a password of length 8-10 characters. He said the length could be increased to 80-100 character. This scheme presented a user password that was not valuable to immediate shoulder surfing for not musically avoided attackers who may hear the tune but able to play it as long the tempo of the tune can be inferred from the tune not the key strokes. He also introduce the piano windows position change to reduce misuse by tracking spywares and shoulder surfing attack. He associated the piano keys to a unique secret code each so that a basic mapping table stores that codes to piano keys in a database. If multiple keys are chosen by the user a bit use AND bit use OR operation are used for white keys + black keys (disimilar) and or white + white or black + black keys (similar) selections respectively. He further converted these respective but unique code into ASCII codes for temporary processing.

The music/tunes generated are not stored only the output string generated with the key secret codes are stored and hassled, the output device for interactions with piano can be a mouse keyboard or acceptance input device on a computer.

Although the work offers a great advantage of memorization which a majorly essential in user password convenience, it has not been deployed on mobile phones and if so vulnerable to easy to guess attacks by music oriented attackers, also a recording of the expected music allows the attacker to get exact key strokes on the piano keyboard without carrying out shoulder surfing since, the key to code mapping is fixed and an ASCII representation mapping is possible very the system vulnerable to ASCII code generation attack.

These passwords are seen to be vulnerable in different areas. In this paper attempt to build a password for mobile device based in the easy memorization characteristic of music.

3.0 The Design Architecture

The general frame work of our designs was adopted from the architecture given in [9] but with our specific parameter as illustrated in figure 1.

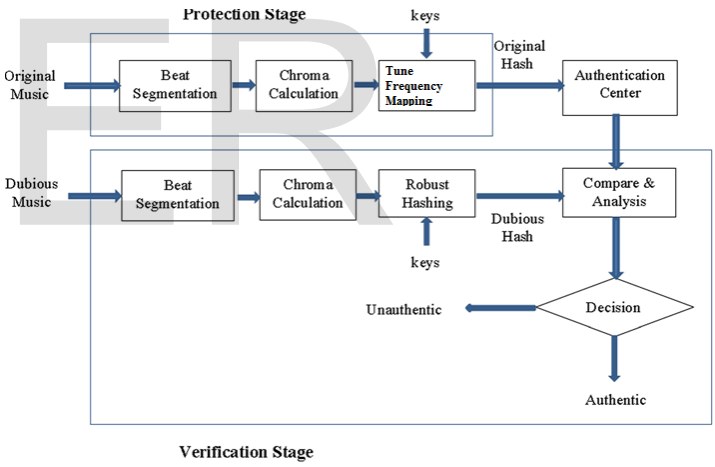

Figure 1 Architecture of the music wave toke authentication

The architecture has a protection stage and verification stage; these stages have in the then sub stage such as conversion of an original music into keys and then verification of the keys during authentication process.

This architecture was manipulated only to music key generating, introducing a level of independence on the music to key generation based on frequency of key stokes for example the length of press in a key determines the generated code on the key. The frequency been the key parameter for the generated

code in addition to a matrix based mapping table as shown in equation (1) matrix representation of key to time mapping

The protection stage:

The music tune generated is first sequenced based on a beat detection system, this system records every sound and corresponding second sequence if similar to zeros and ones, so that a system of 10 or 01 following quantum computing which is used to generate the keys hence when a user has less than the expected or more than or not paly the tune with the exact length of the original music the generated key does not mapp to an already existing keys in an effort to verify the sematic meaning of music content, a chrome which has been usually used in music content analysis as the key feature is used to characterize the progression of main melody and harmonics.

Chroma also called a pitch class profile is a frame-based representation of music signals, where the full spectrum is pyeited into 12 semitones classes intented in an octave to reflect the distribution of music notes. So that 12 dimensional chroma feature of one frame is calculated as shown in equation 2

$$Xpcp(k';n) = \Sigma k:p(k)= k' X_{STFT}(K,n)$$

Eqn 1

Where STFT is short time Fourier transform

Xpcp(k';n) and $X_{STFT}(K,n)$ are the chroma feature and magnitude spectrogram of music signal x(n) respectively , n is the time index and k/k' are the frequency indices

The key database is generated using a matrix of alphabets and numbers. We develop system of alphabets such that the alphabet pool consist as shown in equation 2

2^{26} combinations of which

26 Capital Letters

26 Lower case letters

Where

$\alpha 26^{25}$ is combination of capital letter and small letter subscript

$\beta 26^{25}$ is a combination of small letter subscript and capital letter

$\gamma 26$ is collection of capital letters only

$\varrho 26$ collection of small letter only

$\delta 26^{F10^9}$ combination of capital letters with numbers

$\tau 26^{F10^9}$ combination of small letters with numbers

$f10^9 \Rightarrow f10^9$ is the possible combination of 0-9single or multiple

So that the key becomes

$$\text{Key } k_D = \alpha 26^{25} + \beta 26^{25} + \gamma 26 + \varrho 26 + \delta 26^{F10^9} + \tau 26^{F10^9}$$

Eqn 2

Each of the symbols representing the particular key clause

This key pool is them used to map the music tune on to the bits which can be 01 or 10 or 1 have been generated and a multiplication of the generated matrix done by with an identity matrix the output of the new matrix is then mapped to the member of the key pool based is rule pseudo-randomization. When this is done the remit is stored and the output at all times gives the same result for all consistent music bit entered

4.0 IMPLEMENTATION OF THE DESIGN

The system was designed on a simulated phone using java; this system used a piano keyboard with two white keys and two black keys as shown in figures 2,3,4,5,6,7,8. The system was hence using several combination and showed that it has resistance against Shoulder surfing attack.

The system was designed on a simulated phone using java; this system used a piano keyboard with two white keys and two black keys as shown in figures 2,3,4,5,6,7,8. The system was hence using several combination and showed that it has resistance against Shoulder surfing attack.

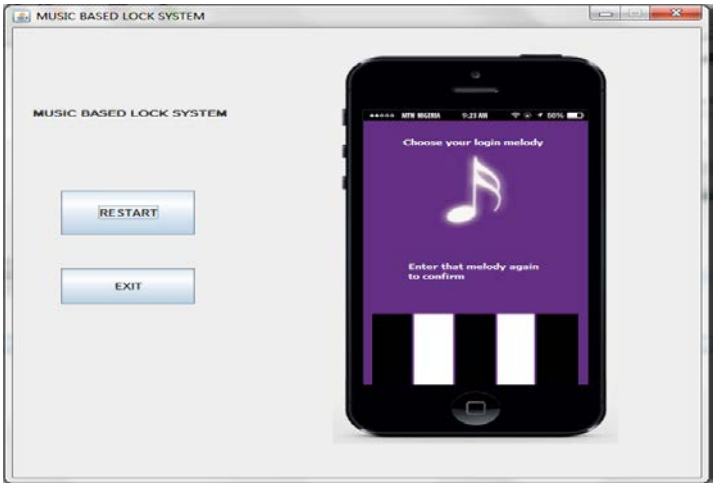

Figure 2: Chosen Melody Validation

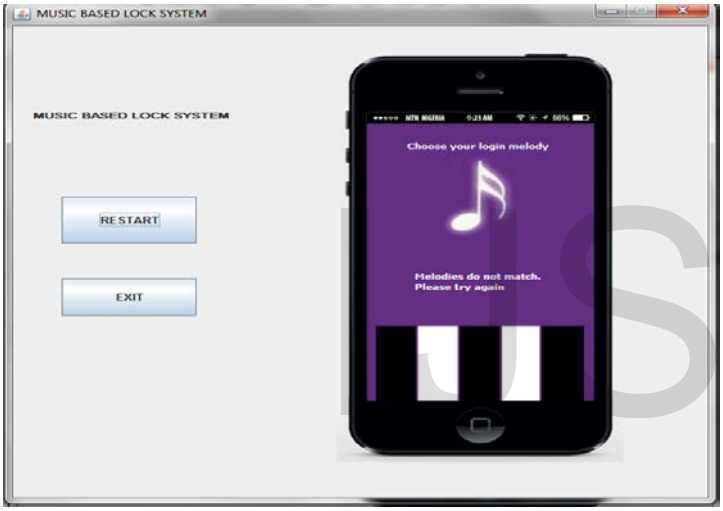

Figure 3: Mismatch Melody

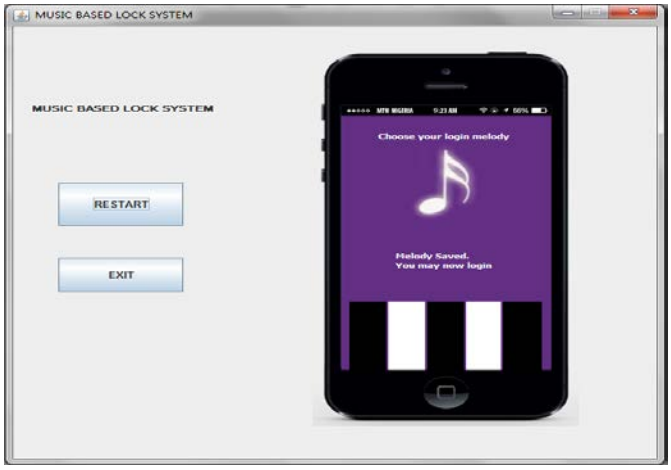

Figure 4: Confirm Melody

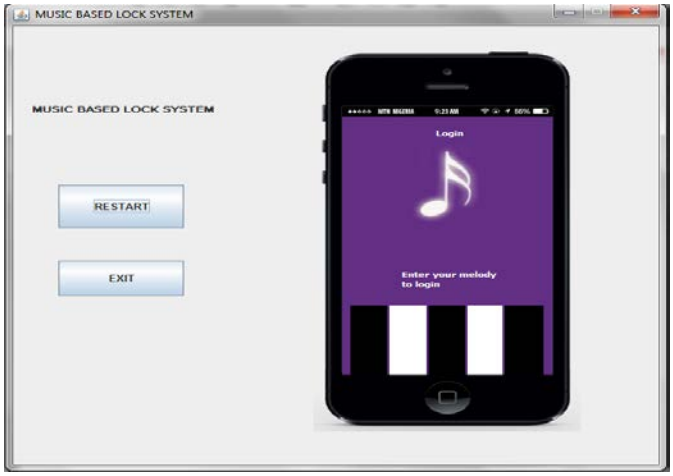

Figure 5: Login with melody

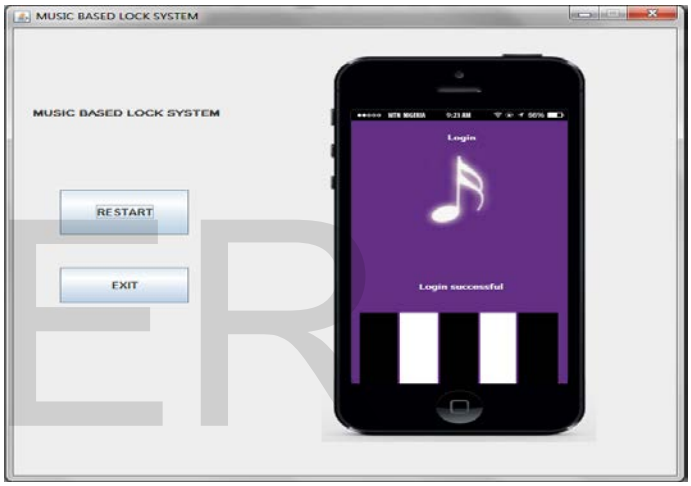

Figure 6: Login Successful

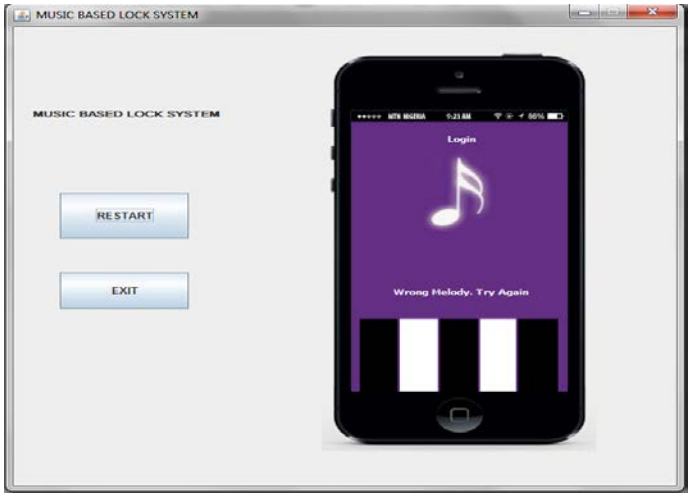

Figure 7: wrong melody

Figure 8: Home Screen

5.0 Conclusion

This report also showed in comparism to that of [6] design that the keyboard makes it less vulnerable dictionary attack although the protection processing requires a longer computation time.

Acknowledgment

We acknowledge the research assistance of Badmus Halimat Bola

Reference

[1] Alqahtani Abdullah Saleh; "Security of Mobile Phones and their Usage in Business" International *Journal of Advanced Computer Science and Applications, (IJACSA) Vol. 4, No. 11, 2013*

[2] Oyinloye, O. E, A. I. Fasiku, B. Alese, A. Folake; "Development of enhanced token using picture password and public key infrastructure mechanism for digital signature" *International Journal of Computer Science and Information Security*, Vol. 9, No. 7, 2011

[3] Hayashi, E., O. Riva, A. J. Brush, S. Schechter; "Goldilocks and the *two* mobile devices: going beyond all-or-nothing access to a device's applications" proceedings of the 8th symposium on usable privacy and security (p.2) ACM 2012

[4] Samson S. and R. J Zatorre , "Recognition memory for text and melody of songs after unilateral temporal lobe lesion: evidence for dual encoding" *Journal of experimental psychology; learning memory and cognition* 1991, Vol 17 No. 4 pp 793 -804

[5] Wallace Wanda T. "Memory for Music: Effect of Melody on Recall of Text" *Journal of Experimental Psychology: Learning, Memory, and Cognition* 1994, Vol. 20, No. 6, M71-M85

[6] Kumar Naveen; "User authentication using musical password" International Journal of Computer Applications 2012 vol 59 No.9

[7] Ratha N and S.Karthikeyan; "An Evaluation of Fingerprint Security Using Noninvertible Biohash" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011

[8] Penny Khaw**; "**Iris Recognition Technology for Improved Authentication" SANS Institute 2002

[9] Li Wei, Xiu Zhang and Zhurong Wang**;**"Music content authentication based on beat segmentation and fuzzy classification" EURASIP Journal on Audio, Speech, and Music Processing 2013,

[10] Mohammed E. F, Vishal M. P, Rama C; "Face-Based Active Authentication On Mobile Devices"; Center for Automation Research, University of Maryland, College Park, MD 20742, 2014

[11] Giray Sait Murat; "Data and Endpoint Security in Mobile Computing" 6th International Information Security & Cryptology Conference Uluslararasi, 2013

[12] Ashland M.A, "The broad reach of biometrics: Fingerprint recognition and mobile security" fairpoint group white paper, Document FPG 2008-435.1, 2008

[13] Anil K. Jain, Arun Ross, And Salil Prabhakar, "An Introduction To Biometric Recognition" IEEE Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1, January 2004