Track Me & Unlock: Secured Mutual Authentication System of Integrating Phone Unlock & Women’s Safety Application using MEMS

S.Vengaten1, M.Wilferd Roshan2, Dr.S.Prince Mary3 and D. Usha Nandini4

1[1] [2] Student, Department of Computer Science and Engineering, Sathyabama University
2[3] Assistant Professor, Department of Computer Science and Engineering, Sathyabama University, Chennai,
3[4] Assistant Professor, Department of Computer Science and Engineering, Sathyabama University, Chennai,
princemary26@gmail.com

Abstract. In the Existing System, Mobile must be unlocked before using. The widely usage of unlocking types are PIN, password and graph. In the Proposed System, we propose a novel token-based mobile device unlocking approach: transferring the authentication state between two devices by briefly shaking them conjointly. In this system; we propose 4 attributes for phone unlocking. 1. Hand waving pattern in mobile, 2. Creating information from embedded hardware through Bluetooth, 3. MEMS waving pattern by the hardware device, 4. Synchronization of both the device. The unlocking pattern of the mobile will be changing every time for safety reasons, It will be changing randomly. The major advantage of this system, even if hacker knows one of the above specified unlocking password, he have to provide answer based on the required pattern so this is more secured application. We also implement Women’s Safety application along with this implementation. We include two patterns for this application. Pressing the switches in the hardware or Phone’s waving pattern is matched immediately system will understand that Women safety application is initiated. GPS is initiated to save the women by sending location info both to the Guardian and Police.

Keywords: shaking them conjointly, hand waving, synchronization, changing randomly, answer based, GPS initiated.

1. INTRODUCTION

The unlocking mechanism in mobiles is PIN, graphical pattern and password, swipe. Biometrics approaches most widely used in mobile devices which includes fingerprint scanner faces detection, or voice detector. The security level of biometric is very low, and easy to access. Biometrics has to be changed, which decreases the use of leakage theft. In addition to biometric features, hardware helps to find and process biometrics on mobile phones is often proprietary. Unlocking techniques are rarely used on mobile phones, in contrast to knowledge-based authentication and biometrics. Many proposed ideas so far are based on token proximity and device to perform the unlock.

There is more possibility to hack the device and can unlock when the user is near to the attacker. For example, with Wi-Fi or Bluetooth-based techniques it might be sufficient to be in the same room with the user to successfully unlock the device. When the hacker is near to the user he will be to access over the mobile phone, there is a chance unlocking the mobile immediately will be possible before leaving the scene. While using token-based authentication user is required with a token, when they want to use their mobile phones. Depending on the token location, it could be possible to obtain control over token and device at same time, and later apply the token to unlock the
device. In case of theft, if token itself is locked to prevent illegal usage, the entire issue is moved from the mobile device to the token a sun locking the token could be done using knowledge-, biometrics or token based authentication. We propose a token-based mobile phone unlocking technique to address the above problems:

- By shaking the device conjointly there is a transfer in action station between two devices. This idea is that personal mobile can be unlocked in different ways each time; one could act as a token, allowing transferring authentication state between devices.
- We are going to provide four types of unlocking by creating we can make sure that the device is protected properly. The security can be advanced by adding some security questions so that if people access our device with permission he cannot pass through the security question. The four types of unlocking system differ from each other hand waving, knock, using MEMS, Bluetooth device.

![System Diagram](image)

**Fig.1: System Diagram**

Fig.1 shows the flow diagram of women safety and unlocking with the use of MEMS sensor and hand waving principle. Here there is location tracking, Voice recorder, and Image capture during emergency.

2. PROPOSED SYSTEM

We propose a idea based on mobile device unlocking types, sharing the action state between two devices by shaking them conjointly. The key plan is that personal mobile devices can remain unlocked for different time of period; one could act as a token, allowing sharing action state between two devices. For example, a mobile device should lock by its own as soon as it put aside while a smart watch will remain unlocked as far it is strapped to the wrist and automatically lock by itself when removed. Example: unlocked once in the morning when attached to the wrist and automatically lock by it when removed.

In this system; we propose 4 attributes for phone unlocking. We need to construct Embedded Hardware consisting of MEMS Accelerometer Sensor for identifying Phone’s shaking pattern, Bluetooth hardware for Communication, 2 Switch for Signalling the Phone devise. Using this above system user can set 4 types of password for phone unlocking.

- Hand waving pattern,
- Creating information from embedded hardware through Bluetooth
- MEMS waving pattern by the hardware device
- Knock-knock. There will be a change of unlocking pattern every time during unlocking.

The major advantage of this system, even if hacker knows one of the above specified unlocking password, he have to provide answer based on the required pattern so this is more secured application. We also implement Women’s Safety application along with this implementation. We
include two patterns for this application. By pressing the switches in hardware or by waving the mobile is matched immediately system will understand that Women safety application is initiated. GPS is initiated to save the women by sending location info both to the Guardian and Police shown.

Fig.2. Hardware Device

Fig.2 is the hardware device with the Bluetooth and MEMS sensor connected to the board. This is used to unlock device.

3. IMPLEMENTATION:

In the module we create an application for secured authentication. The android application is created and then installed in User’s Android Mobile Phone. The first page in this application consists of user registration process. We create the User login page by Button and Text Field class in the Android studio. User has three types of registration first they have to register their Name, Guardian Number, Police Number, Ambulance Number, Alternate number to send the message. Secondly have to register four types of unlocking system. Finally some static questions will be asked by application for security reasons. We use MEMS, Bluetooth and switch to unlock the device.

MEMS-Micro Electro Mechanical Systems. MEMS is define as combination of a number of micro components on single chip. This allows micro system to sense and function the environment. MEMS will analyze the motion to the hardware and image of MEMS is shown in Fig.3. Bluetooth will transfer the value to the server to verify the values that we already registered. Switch is a button to unlock the device when we press that button from hardware kit it will generate the value and that value will send via Bluetooth.
Fig. 3: MEMS SENSOR

Switch based authentication is a smart hand hold device is connected with user. A switch is attached with that device with Bluetooth. When the user press that switch it will generate a value to unlock. But mobile will not unlock after the switch is pressed. The generated value will send through Bluetooth and that value will be verified by the system after that only the device will unlock.

Synchronized authentication is both the MEMS and the hand waving should synchronize each other. That is we already register the mobile tilde and the motion of the Mims’s if the user when unlock the mobile it will read both mobile tilde and MEMS motion. After the synchronization of the both device mobile will unlock automatically.

WOMEN’S SAFETY-In this, unlocking system will make only in mobile. In home page of application two buttons will be displayed on the screen. One for emergency and another for forgot password. If the user forgot the password a four set of questions will be asked by the application. After the correct answers givenby the user the mobile will unlock. If the answer is not correct mobile will consider the system is hacked by someone so a message is sent to alternate number of the user. Another button is for emergency if user press the button a GPS location is sent to the register mobile number. If she had physical harassment message will be sent to local guardian and police. Implementation result screens are shown in fig.4.

Fig. 4. Implementation

4. CONCLUSION

We provide four types of unlocking system to the user. This system will give more security than the existing system. As we mentioned above we provided better security system for android devices. By including the four types of unlocking systems, now it is made sure that android device can be
unlocked and secured. Since security questions have to be inserted in this unlocking systems this application is made sure that the user’s mobile cannot be breached easily. And also the above proposed system provide a security to the girls when their in emergency situation, GPS is initiated to save the women by sending location info both to the Guardian and Police so that the harassment can be controlled.

REFERENCES

[1]. R. D. Findling, M. Muaaz, D. Hintze, and R. Mayrhofer, “ShakeUnlock: Securely unlock mobile devices by shaking them together,” in Proc. 12th Int. Conf. Adv. Mob. Comput. Multimedia, Dec. 2014, pp. 165–174.
[2]. M. Swan, “Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0,” J. Sensor Actuator Netw., vol. 1, no. 3, pp. 217–253, Nov. 2012.
[3]. Z. Ni, Y. Shi, N. Ansari, and S. Wei, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[4]. W.Hong, T.Chen and H.Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE. Signal process. Lett ,vall.19,No.4,pp.199-202,apr.2012.
[5]. Christian M. Toader,”User authentication for Pico”IEEE,No.4,pp.199-202,Apr 2011.
[6]. Bandaru R, Albert Mayan J ( 2016) ,"Novel approach for whole test suite generation using metamorphic relations",Indian Journal of Science and Technology, Vol 9,No.10, pp.1-7.
[7]. AntoPraveena M.D., Joseph Manoj R, Shanthi V (2014) , "An authentication method for secure web services access with preventing tautology type SQL injection ",International Journal of Applied Engineering Research,Vol.9, No.20,pp. 7531-7543.
[8]. Mary S.Prince, Dr.Baburaj.E, "Constraint informative Rules For Genetic Algorithm-Based Web Page Recommendation System", Journal Of Computer Science 9 (11), pp:1589-1601,2013.
[9]. D.Usha Nandini, Dr.Ezil Sam Leni, A Survey of the Existing Shadow Detection Techniques, International Conference on Control, Instrumentation, Communication and Computational Technologies, pp.175-177, 2014.