International Conference on Applied Science, Technology & Management
Mahratta Chamber of Commerce, Industries and Agriculture, Pune (India) ASTM 2018
10th February 2018, www.conferenceworld.in ISBN: 978-93-86171-99-3

An Enrichment of Token Based Scheme for Women Protection Using MEMS Approach

Ms. R. Poorvadevi[1], Spoorthy Reddy Jarugu[2], P.Vamsi Priya[3]

[1]*Assistant Professor, CSE Department, SCSVMV University, (India)*

[2, 3] *UG Student, CSE Department, SCSVMV University,(India)*

ABSTRACT

Nowadays, women security is playing a vital role in the domain specific environments which specify the significant role in the public. However, lots of security components, approaches, privacy tools and techniques will come with the new scope, still the women security problem is not completely eradicated. The major security problem is that, how the security functions and factors are enabled in the wireless access environment. If women are suffered with the problem then, immediately how the complaints are passed to the police station people to take the desired action. For this strategy, the proposed work of novel based token system has been generated to prove the authenticity and betterment of this work by using the MEMS approach. Through is approach, women harassment and other complaints has been forwarded using the sensors to nearby police station officers and they will provide the optimal solution. This approach has been performed through the mobile phone signaling with the use of hardware devices to detect and rectify the problem of women annoyance.

Keywords: GPS, Waving pattern, MEMS accelerometer, Embedded Hardware, NFC, Mobile Unlocking, Signaling ratio.

I.INTRODUCTION

The most widely used mobile knowledge-based unlocking mechanisms are PIN, password and graphical pattern. All of them increase the cognitive load on the user and require a certain time to enter the secret knowledge which might be cumbersome due to small user interfaces on mobile devices. Furthermore, knowledge based unlocking approaches are vulnerable to shoulder surfing attacks secret, and smudge attacks. Attackers screening the display after the user authenticated using a graphic pattern to observe the residual smudge that might remain on the display, thereby observing the unlocking secret. Biometrics-based approaches most commonly used on mobile devices include fingerprint (e.g., Apple Touch ID), face, or voice. In addition, hardware used to capture and process biometrics on mobile devices is often proprietary, which makes identifying and analyzing potential security issues difficult. In contrast to knowledge-based authentication and biometrics, token-based unlocking mechanisms are rarely used on mobile devices. Most approaches proposed so far are based on proximity of token and device to perform the unlock. As attackers are likely to be close to the user when obtaining control over the mobile device, an immediate unlock would be possible before leaving the scene. When using token-based authentication, the token needs to be brought by users everywhere they potentially want to use their mobile device. Depending on where the token is kept, it could be possible to obtain control over both token and

device at once and then use the token to unlock the device. If the token itself is locked to prevent illegitimate usage in case of theft, the whole problem is transferred from the mobile device to the token as unlocking the token itself again could be done using knowledge-, biometrics or token-based authentication. The approach is on shaking mobile devices conjointly to establish a secure channel between them, it focuses on shaking as a secure trigger mechanism to transfer authentication states from a token device to another device over a pre-established secure channel.

II. RELATED WORK

As per Muhammad Yasir Sarosh, "In Pakistan, working women often become victims of harassment during traveling which exacerbates uncertainty and hesitance among other workingwomen regarding their security". This paper discusses the android application, Mehfooz Aurat (safe woman), which developed to support the lower socio-economic income bracket of working women who use public transport. The key features include safe routes, emergency alerts and audio recording with a unique self-defense section. The app has text based output in the national language, Urdu, which makes it accessible to the majority who are unfamiliar with the English language. Our usability tests reveal that the system is perceived to be useful and easy to learn; with brief learning, even the uneducated workingwomen were able to benefit from the application. [1]

As per Janet E.Burge, Gerald C.Gannod, Maureen Doyle, Karen C.Davis, this paper describes our experience running "Girls on the Go: The Mobile Computing College Experience." It is decided to do a residential summer camp for HS-age girls to achieve two goals: to encourage our campers to attend college and to interest them in computer science as a possible career option. It is centered the camp around the design of a zoo themed research tool where campers designed a mobile application to be used by researchers to document and study animal behavior. Post-camp surveys gave statistically significant results indicating that the camp increased the girls confidence in performing computer science and understanding what computer scientists did. [2]

So, from the above approaches the various security measurements and metrics have been used in a partial manner. It will specify the components can runs under the specific environment which decides the security and privacy factors of the women safety system enabled and processed in the proposed system.

2.1 Limitations of the Earlier Approaches:

Mobile users have to unlock them before usage. Authentication conceptually is divided into knowledge-, biometrics-, and token based-authentication. Most widely used mobile knowledge-based unlocking mechanisms are PIN, password and graphical pattern. Some of the drawbacks listed as below:

- System doesn't consist of any proper authentication.
- There is no preserved security mode for lock or unlock.
- No alert system for guardian and police.

III.PROPOSED WORK

The proposed work of "novel token-based mobile device unlocking approach" specifies the various functionalities which include offering the authenticity and authorization based control over the women sector group. This approach is transferring the authentication state between the two devices by briefly creating the security peripheral devices in two different end systems. The major key idea is that, personal mobile devices can remain unlocked for different time zone. one could act as a token, allowing to transfer authentication state between devices. For example, a mobile phone should lock itself as soon as it is put aside while a smart watch could remain unlocked as long as it is strapped to the wrist and automatically lock itself when detached. The smart watches could be unlocked once in the morning when attached to the wrist and automatically lock itself when detached.

The proposed model consists of 4 attributes for phone unlocking. The need is to construct Embedded Hardware consisting of MEMS Accelerometer Sensor for identifying Phone's shaking pattern, Bluetooth hardware for Communication. Switch for Signaling the Phone devise. Using this above system user can set 4 types of password for phone unlocking. The unlocking patterns are:

- Hand waving pattern in the phone
- Switch signal from Embedded hardware via Bluetooth
- MEMS waving pattern from the Hardware
- Both the Devices synchronization.

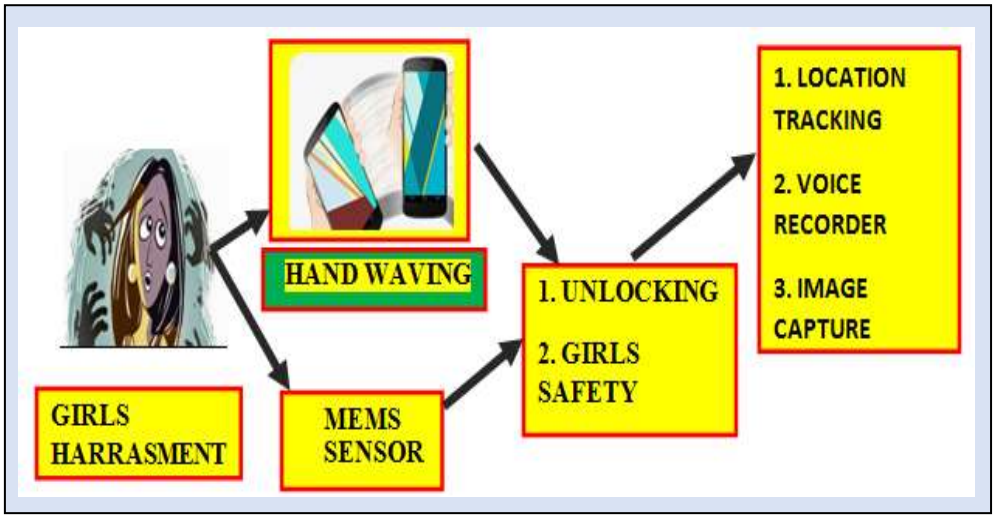

Figure: 1.1 Depicting the Architecture of Proposed Model

In the proposed model (figure 1.1) user phone's unlocking pattern will be randomly changed. 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. It also implements women's safety application along with this implementation. These approaches include two patterns for this application.

Either pressing both the switches in the embedded 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 information both to the Guardian and Police from this desired action can be taken for the given problem against the complaint received from the concern location.

IV.IMPLEMENTATION WORK

In this approach, constructing an embedded hardware control has been deigned to monitor the various activities. MEMS accelerometer sensor can be used to identify phone's shaking and waving pattern, communication process over the Bluetooth hardware devices. The various two signaling switches are configures in the phone device. The security components are enhanced in the betterment process of women safeguard system and using the phone device additional factors it will verify the credentials of the secured access environment. The various access specific constraints also used to identify the suitable hardware control over the novel token based approaches.

4.1Operational Procedures of an Implementation Work

The system allowed the user to set the options and security parameters of the specific access control devices. The various protection based peripherals can be used to iterate the process of controlling the signaling inputs. The proposed system can set the four distinct set of passwords are preferred for phone unlocking operation. The various inputs specific operational process was given below:

- Creating hand waving pattern in the phone devices are enabling the security pattern for the private location.
- Switching the signaling input values form the embedded hardware via Bluetooth devices.
- MEMS waving pattern can be enriched and optimized in the hardware controller.
- Enabling the services of Device synchronization process to find out the access rights of the phone when it is in locking state.
- Access permissions are denied in the hacker entry's location.

There will be randomized changes in the unlocking pattern values. The major advantage of this proposed work is unlocking pattern will optimize the values of randomly generated input pattern outcomes. From this, attackers are able to steal the specific unlocking password, for accessing the entire set of data values (or) pattern values hackers need to answer for the hand waving based signal specific application.

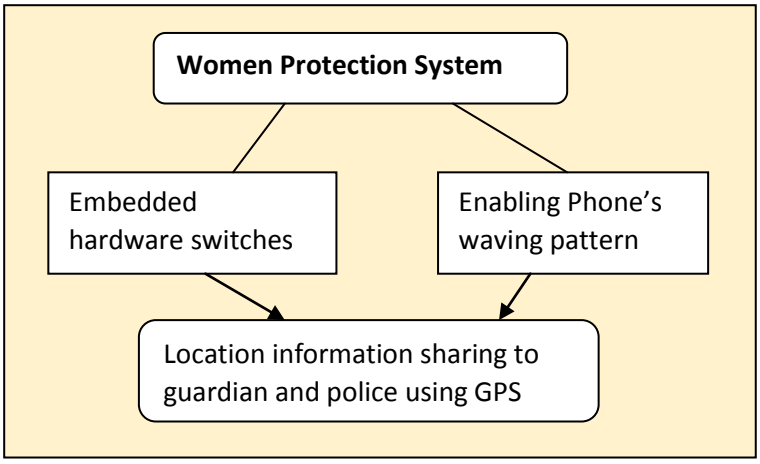

Fig: 1.2 Illustrating the comparison of phone's waving pattern signal

From an above figure 1.2 it is proved that, the two major functional components are used to iterate the process the women harassment approach. Embedded hardware can be majorly used for the system optimization level based operations. The merit of this approach can specify that, multiple security options do not allow hackers to proceed the further authenticity steps in the protection system. Enabling smart device synchronization needs to find out the actual waving pattern values.

V.RESULTS AND DISCUSSIONS

From the analyzing perspective of women security system, it is enhancing the security operational outcomes of the various access specific constraints. By applying this technique, women are protected in the emergency situation. The various components are gathered in this approach in order to specify the security components are used to optimize the security control over the women protection system environment.

Table: 5.1 Processing of Hand waving Pattern Values

Women Location Tracking Status	Embedded Hardware Control	Phone's Hand waving pattern Matching Values	Optimized Value Efficiency
Yes	Switched	Synchronized MEMS value	Acceptable
Yes	Iterated	MEMS Tracked	Acceptable
Yes	Migrated	Segmented	Moderated
Yes	Optimized	Isolated	Initiated
Idle	Changed	Checked	Mode Changed

The above table 5.1 illustrates the functional flow of women protection system. The various security based componnets are processed in the proposed model with an elements of embeded hardware control and tracking

thehandwaving signal pattern values. It is identifies that the optimal efficiency was obtained in the implemented approach

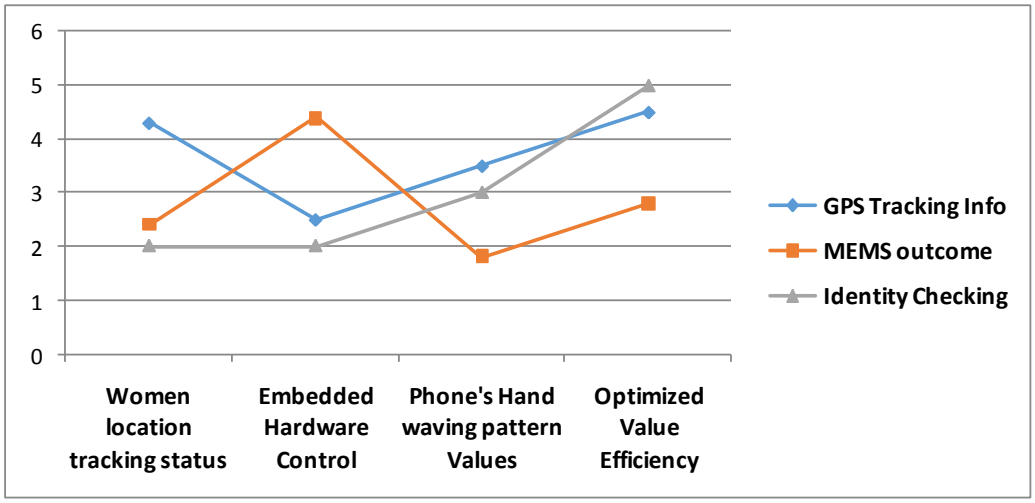

Figure: 1.3 Experimental Outcomes of Women Protection Approach

From an above figure 1.3 it is identified that, the various security components are taken into consideration for proving the better efficiency outcomes of the women harassment problem. It will be operated with the help of enabling embedded hardware device control and MEMS hand waving pattern based signal values.

VI.CONCLUSION

Thus the proposed work will provide the enough security components to the girls who suffering from the critical situation. The unlocking system will provide enough security control in the user location and also enriching the security operational outcomes are monitored and managed by the service security elements.

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 Networking., vol. 1, no. 3, pp. 217–253, Nov. 2012.

[3] G. Thomson, "BYOD: Enabling the chaos," Netw. Secur., vol. 2012, no. 2, pp. 5–8, 2012.

[4] B. Morrow, "BYOD security challenges: Control and protect your most sensitive data," Netw. Secur., vol. 2012, no. 12, pp. 5–8, 2012.

[5] S. N. Abdulkader, A. Atia, and M.-S. M. Mostafa, "Authentication systems: Principles and threats," Comput. Inf. Sci., vol. 8, no. 3, pp. 155–179, 2015.

[6] L. Gorman, "Comparing passwords, tokens, and biometrics for user authentication," in Proc. IEEE, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[7] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy, "Modifying smartphone user locking behavior," in Proc. 19th Symp. Usable Priv. Secur., 2013, pp. 10-14.

[8] A. Adams and M. A. Sasse, "Users are not the enemy," Commun. ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[9] L. F. Cranor and S. Garfinkel, Security and Usability. Sebastopol, CA, USA: O'Reilly Media, May2008.

[10] P. Bao, J. Pierce, S. Whittaker, and S. Zhai, "Smart phone use by non-mobile business users," in Proc. 13th Int. Conf. Human Comput. Interact. Mob. Devi. Serv., 2011, pp. 445–454.