International Journal of Engineering Research and Reviews ISSN 2348-697X (Online)
Vol. 8, Issue 1, pp: (6-10), Month: January - March 2020, Available at: www.researchpublish.com

ACTUALIZING A MULTI INTEGRATED IDENTITY MANAGEMENT MECHANISM FOR CONTROLLING ACCESS IN AUTOMOBILES

[1]Dawson john kwao, [2]Dr. Thomas Yeboah, [3]Michael Osei Boakye

[1]Kwadaso College of Agriculture, Kumasi, Ghana
[2]Christ Apostolic University,
[3]NJUST

Kwaodawson1@yahoo.com, thomyebs24@gmail.com, Michael.ob@njust.edu.cn

Abstract: **Identity Management is a combination of procedures and innovations to oversee and secure access to an Information Technology infrastructure. A user authentication in an automobile is a critical security issue due to their unattended and improper deployment as most automobiles are outfitted with limited computing power and accordingly verifying users has now been a fundamental security concern. The methodology employed in this paper is Method for Architecting Secure Solutions (MASS) minutiae-based matching module for finger print identification. The most ordinarily utilized identity management tool is the secret key and username approach which ends up plainly weakened when the more prominent verification of the user identity is required. In this paper, a multi-factor client user identity management paradigm is proposed named Name, Age and Biometric (NAB) which is a mobile application embedded on a microcontroller. This framework has the capability of confirming the Name, Age and Biometric (fingerprint) of the user. The point is to give a layered barrier and make it more difficult for unauthorized user to gain access to automobile, control age eligibility to access the automobile and control theft cases.**

Keywords: **MASS, Identity Management, Biometric.**

1. INTRODUCTION

Identity Management according to Slone (2004) is defined as the quality or condition of being the same; absolute or essential sameness, oneness. To be uniquely identified form someone in this era is based on identity.

There is continuity in automatic electronics which is likely to end now but to move to a more advanced level. Nowadays, modern automobiles are manufactured with multiplicity of microcontrollers that are networked together via various communication approaches with diverse properties. These automotive communications are linked to several important components of the automotive like the brake system, airbag, the control board and the engine Wolf et al(2004).

Security of automobiles are becoming paramount to be able to cater for theft cases and also control the situations where as a result of curious children in attempt to practice what they observe.

The continuous integration of advance but unsecured automotive control systems with new automobile multimedia networks like Media Oriented System Transport and Global System For Mobile Communication as well as Bluetooth causes various security risk.

This paper presents a more secured and layered barrier approach which makes it more difficult for unauthorized user to gain access to an automobile, control age eligibility to access the automobile by using NAB. This is made up of a mobile device which provides an interface to accept the name of the owner, the age of the owner and finger print of the owner.

When buying the automobile the individual's name, age and finger print is configured on the mobile device as a security to be the only one to be able to have access to the automobile but can be reconfigured upon fulfilling the initial configurations. After fulfilling all authentications the door of the vehicle will open automatically with a beep sound signaling successful identification. If two of the authentication fails (name and age) the door will not open but gives an error message ("NOT THE OWNER") but if the two are successful but the biometric authentication fails the automobile gives buzzer alert.

2. RELATED LITERATURE

According to Squicciarini (2011) the use of VANET known as the Vehicular Ad-hoc Network is a growing trend in future consumer automobile product development. It enables exciting applications ranging from road safety to traffic control, up-to mobile entertainment Girinath D, (2010). A number of major players in the auto industry, telecommunication carriers and consumer computer product manufacturers have made some early efforts on this subject. Current prototypes like NOW (Network on Wheel) (Jerome et al. 2007), California Path (Matt F. 2004) and SeVeCom (Zhang F and Zhang J. 2014) have already provided workable testing-models for real-world use. In spite of all these, there arise a large number of challenges in VANET such as provisioning of QoS, high connectivity and bandwidth and security to vehicle and individual privacy.

Dimple et al (2015) in their work proposed the use of smart card to get access and ignit vehicle upon successfully fulfilling the steps listed below

- Checking to if the drivers license is valid.
- Verify if the license is learner
- Authenticate if the driver's license is blocked.

Irrespective of how this mechanism is able to check valid driver's license, the level of the driver's license and if the driver's license is blocked or not still is not able to identify the owner of the vehicle as such any individual can enter any body's vehicle at that persons comfort.

According to Farooq (2014) they proposed a system which combines RFID technology and biometrics to accomplish the required task. When the RFID reader installed at the entrance of hostel detects a number, the system captures the user image and scans the database for a match. If both the card and captured image belong to a registered user, access is granted; otherwise the system turns on the alarm and makes an emergency call to the security van through GSM modem. In this way, the suspicious persons can be caught. This system failed to consider monozygotic twins where their images are the same. In such a situation there can be misplaced identity as such does not hold for all situations.

3. OVERVIEW OF NAB

NAB system is made of three phase authentication levels provided using mobile device with an application provided by the manufacturer. These are Name authentication, Age authentication and Biometric (finger) authentication. The information that is provided is verified and if valid access is granted for the automobile door to be opened.

NAB APPLICATION

In this project, NAB application is developed which is embedded onto a microcontroller. The main block of authenticated access control for vehicle door system is the NAB application system embedded on the microcontroller which is the heart of the system. The microcontroller is fed with the required input from the various parameters. The various parameters send signals, each to individual pins of the microcontroller. The microcontroller then branches out to any one of the logical paths and delivers the output at one of its pins, which is used by the doors controlling unit. The controller is used to check the authentication process. All the doors are connected to the controllers to control the doors actions. The LCD block is provided for displaying the Name, Age and Fingerprint interface for the holder of the mobile device. Microcontroller verifies the provided personal details in the mobile device. The controller will not accept the Age of the holder of the mobile device if the Name entered is not valid. It also will not allow the holder to enter the Age if the Name is not valid and as such gives an error message" NAME IS NOT VALID" and will not proceed to the biometric verification stage. On any situation where the name and age entered is valid but the biometric fails a buzzer alert will be giving indicating that the individual is able to guess the name and age but not the biometric and so a theft case can be reported.

NAME INTERFACE

This component of the NAB application accepts name of the owner of the automobile both in upper case and lower case alphabets as well as toggle situations. The names should be arranged with surname first followed by the first name while the middle name will be optional. If the answer provided is valid it allows the user to proceed to the next authentication stage. This dialogue box is almost always active anytime the mobile device is touched but goes to the sleep mode after thirty seconds of idealness.

AGE INTERFACE

This phase of the authentication stage verifies the age of the holder of the mobile device. The age is entered as a numeral. If the age entered is lower than eighteen years, the holder of the mobile device is considered immature and an error message "NOT ELIGIBLE" shows on the LCD followed by a beep sound and returns to the name interface.

BIOMETRIC (FINGER PRINT) INTERFACE

This is the final authentication phase which captures the finger print of the holder of the mobile device. The minutiae-based matching module is used in this work. The holder places the thumb on the reader, the Light emitting diodes emits an IR rays and the fingerprint reader captures the image that appears and sends a signal to the microcontroller. If the captured image is valid a beep sound is heard after which the door of the automobile will open. This interface will only emerge if the name and age of the holder of the mobile device is valid. In situation where the finger print is not valid a buzzer alert will be made which is an indication of a theft case.

SYSTEM IMPLEMENTATION AND RESULTS

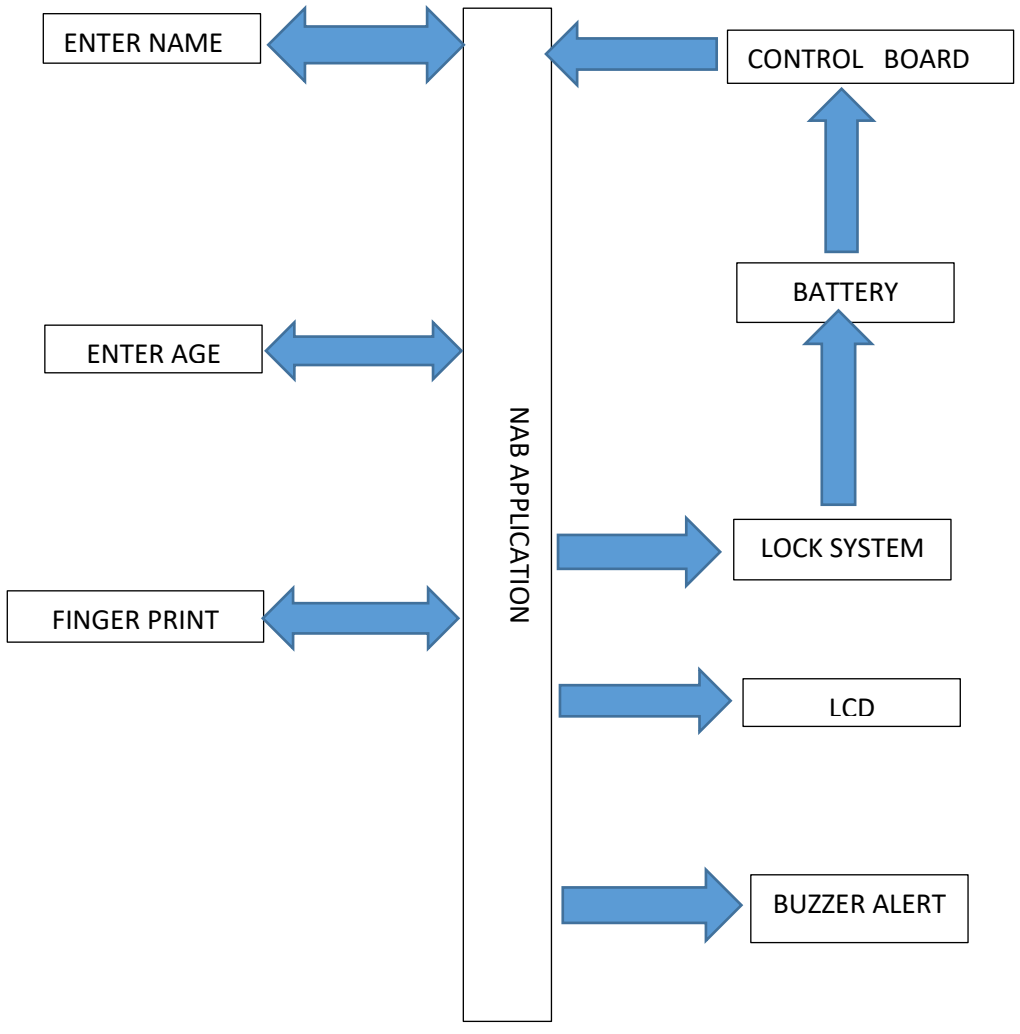

Figure 1. Diagram of systems architecture

In this project one important player is the microcontrollers. This component receives signals in bits to produce results. When the mobile device is active the holder enters the name and if matches with stored name in the system will be verified by the microcontrollers and proceeds to the age interface to accept the age of the holder. If the age is valid after verification will proceed but if not valid and less than eighteen years an error message will indicate on the LCD. The finger print verification interface is then activated to scan the finger print of the holder. If the finger print verification is valid a beep sound is made and the door opens but if invalid a buzzer sound will be alerted signaling theft case. The hardware component of the system is shown in figure 2.

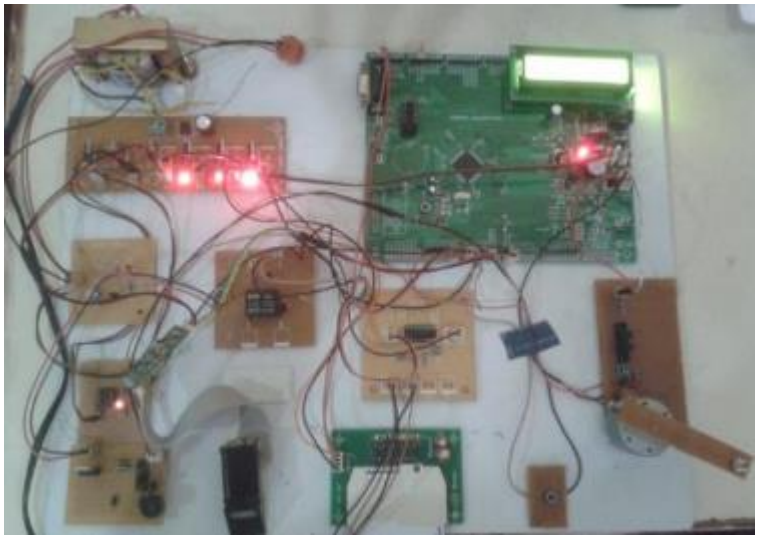

Figure 2. Systems Hardware

If the mobile device is active it will prompt the mobile device holder to enter a name which is embedded in the microcontrollers this will be the results.

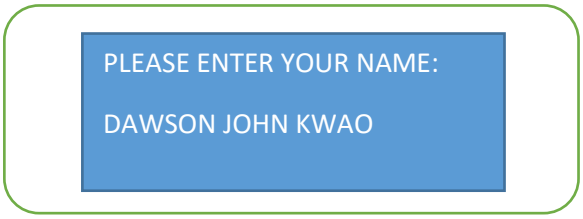

Figure 3: Active mobile device

If the name entered is valid, it proceeds to the second phase for the mobile device holder to enter Age

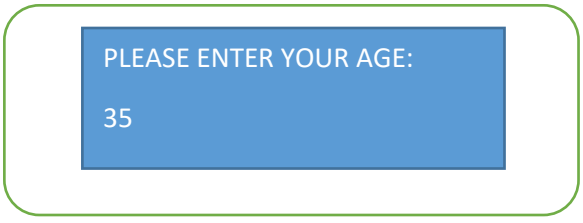

Figure 4: Prompt to enter age

If the age entered is not valid or lesser than 18 this will be the results

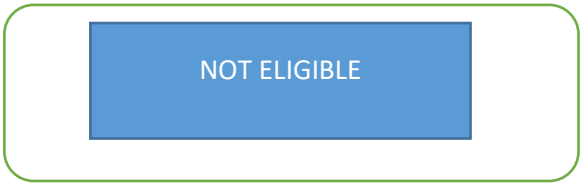

Figure 5: Results of age less than 18

If the name and age are authenticated then the biometric verification will be done. If verified is seen on the LCD it will be followed immediately with a beep sound and the door of the automobile will be opened.

Figure 6: Results of authenticated mobile device holder

4. CONCLUSION

It can be concluded that the application of NAB as an automobile identify management tool will help control the incidence of automobile theft cases since the system will require major fulfillment of age, name and biometric to have access. This approach should be tried on modern automobiles.

REFERENCES

[1] Dimple B., Chary V., Reddy N. and Dileep A.2015. Authenticated Access Control for Vehicle Ignition System by Smart Card and Finger print Technology. *Journal of Electronics and Communication Engineering*, 1(1), pp. 45-48.

[2] Matt F. 2004. *Advances in Cryptology-Crypto 2004.* California, Founding and Former Series Editors.

[3] Farooq U., Hassan ul M., Amar M. 2014. RFID Based Security and Access Control System. *International Journal of Engineering and Technology*, 6(4).

[4] Zhang F. and Zhang J. 2014. *Theoretical Secure Verifiable Secret Sharing with Vector Space Access Structures over Bilinear Groups.* New York, ACM Digital Library.

[5] Girinath D, and Selvan S. 2010. A novel cluster based routing algorithm for hybrid mobility model in vanet. *International Journal of Computer Applications*, 1(15), pp. 35-42.

[6] Jerome F. 2007. *Vehicular mobility simulation for vanets.* Secaucus, Association for Computing Machinery.

[7] Slone, 2004. *Identity Management*, San Francisco,: The Open Group.

[8] Squicciarini A., Lin D. and Mancarella A. 2011. *PAIM: Peer-Based Automobile Identity Management in Vehicular Ad-Hoc Network.* Munich, IEEE.

[9] Wolf, M. A. 2004. *Security in Automotive Bus Systems.* Bochum, s.n.