# Double Authentication Locking System Using NFC Technology and Password

Afiqah Liyana Binti Mohd Jalili
University Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
afiqahliyana92@gmail.com

Delina Mei Yin Beh
University Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
delina@unikl.edu.my

***Abstract*— Electronic Lock System are useful for an organization to use for daily working such as for storage or for entering company to keep the organization are safe from unauthorized person use it for illegal action. With this, an organization can use Double Authentication Locking System Using NFC Technology and Password from being used by unauthorized person without permission. There are several problems an organization to keep the storage are safeness such as unauthorized person easy access the system based on single authentication access and or a person in organization lost the small token or device for accessing the lock system. The aim on this purpose project is to enhance a single authentication access by developing a double authentication access for lock system and an organization have a permission can access it by using the system. Furthermore, this purpose project using Rapid Application Development that been modified. In addition, this purpose project was using Atom software for running the Arduino with the NFC chip and password. When a person tries to get a permission to unlock it, Double Authentication Locking System Using NFC Technology and Password prevent and secure it based on the authentication that apply on the purpose project. In addition, to ensure that only authorized user can unlock and access it.**

***Keywords—component; formatting; style; styling; insert (key words)***

## I. INTRODUCTION

Lock system is used to be a system or device that allow locked and unlocked or serve as tool for securing such as door, lid, drawer, locker or position that implement any access that need permission that called an authorization. In the field of system security, lock system performed as an identification and authentication to claim the information. This process of authentication can be done by providing information, which is something that identifying the user is such as fingerprint, eye, and face and something that user have known or save such as password, PIN or device to detect system.

Nowadays, Electronic Lock as one of enhancement lock system that implement it. Besides, it operated using many types of electronic lock and method for authenticating the system by using RFID, barcode, password, or devices in order to secure it.

However, the current lock system using a single authentication method for accessing. Besides, there any security issue using single authentication. This is because attackers can find a way and method to be used to gain on accessing the lock system illegally.

Therefore, the purpose of this project is to enhance the technology of the current lock system security in the existing system. This project aims to lock and unlock the system and it contains double layer authentication method such as a upgrading the security level of the lock system to make it more secure and prevent from being intruded by unauthorized user. This proposed project is using NFC Technology as a first layer authentication method for accessing and act as a hidden layer for users to access the lock system by tapping the Android smartphones that's been installed with NFC technology chip to the reader NFC. In addition, there will be a combination of the second layer authentication using a password as a second method to identify the right access

## II. RELATED WORK

### *A. Why NFC Technology*

As the technology operates in a very limited range, it is ideal for secure transactions; it even serves as a safeguard against hackers[1]. From the statement above that using NFC Technology implement for the proposed system project are suitable because the limitation range, which is 4cm by 10 cm for exchanging any data through this technology.

More than that, according to NFC Forum "By integrating NFC, devices can support and interoperate with existing contactless card applications and infrastructures. NFC technology will harmonize today's diverse contactless technologies, enabling solutions in areas such as information collection and exchange, Access Control, healthcare, loyalty and coupons, transportation, payments, and consumer electronics." From the above statement, this project can apply the NFC technology because the device with NFC technology can support a system such an access control that mean, this project category as an access control project. Based on the previous problem statement that NFC can be attacked by eavesdropping and data manipulation. Using secure channels such as Secure Sockets Layer (SSL) as a safeguard the transmitted data are encrypted [2]. This will help to protect against the attack. With this, the

project can relate it by secure it using a double layer as an extra the security the proposed system

### *B. Comparison between Bluetooth and NFC*

Bluetooth and near field communication share several features, both being forms of wireless communication between devices over short distances. NFC is limited to a distance of approximately four centimeters while Bluetooth can reach over thirty feet. While it may seem that Bluetooth is superior in this regard, both Bluetooth and NFC technology have their advantages and disadvantages compared to one another and can work together to meet users' needs [3].

NFC technology consumes little power when compared to standard Bluetooth technology. Only when NFC has to power a passive, unpowered source such as an NFC tag does it require more power than a Bluetooth transmission.

The close proximity that devices connected using NFC must be to each other actually proves useful in crowded locations to prevent interference caused when other devices are present and trying to communicate. Bluetooth may have trouble dealing with interference when trying to send signals between two devices, especially when several other devices are in close proximity.

Another benefit of NFC technology comes in its ease of use. Bluetooth requires users to set up connections manually between smartphones and takes several seconds. NFC connects automatically in a fraction of a second, so fast it seems instantaneous. Though the users must be close to one another to use NFC technology, it is faster and easier to set up than a Bluetooth connection.

Bluetooth does still offer a longer signal range for connecting during data communication and transfers. NFC technology has taken advantage of this and can connect two devices quickly, then turn the signal over to Bluetooth so the owners can move further away without severing the connection. The latest development in Bluetooth technology, Bluetooth low energy (BLE) is targeted at low power consumption and uses even less power than the NFC. As the technology increases, Bluetooth and NFC technology may continue to work together, relying on each other to help users meet their data transmission needs.

Table 1 shows the comparison why chooses NFC Technology.

| | NFC | RFID | IrDa | Bluetooth |
|---|---|---|---|---|
| Set –up time | <0.1ms | <0.1ms | ~O.5s | ~6 sec |
| Range | Up to 10cm | Up to 3m | Up to 5m | Up to 30m |
| Usability | Human centric Easy, intuitive, fast | Item centric Easy | Data centric Easy | Data centric Medium |
| Selectivity | High, given, security | Partly given | Line of sight | Who are you? |
| Use cases | Pay, get access, share, initiate service, easy set up | Item tracking | Control & exchange data | Network for data exchange, headset |
| Consumer experience | Touch, wave, simply connect | Get information | Easy | Configuration needed |

### *C. Differences between MD5 and SHA algorithms*

Table 2 : Comparison between MD5 and SHA

| Keys For Comparison | MD5 | SHA |
|---|---|---|
| Security | Less Secure than SHA | High Secure than MD5 |
| Message Digest Length | 128 Bits | 160 Bits |
| Attacks required to find out original Message | $2^{128}$ bit operations required to break | $2^{160}$ bit operations required to break |
| Attacks to try and find two messages producing the same MD | $2^{64}$ bit operations required to break | $2^{80}$ bit operations required to break |
| Speed | Faster, only 64 iterations | Slower than MD5, Required 80 iterations |
| Successful attacks so far | Attacks reported to some extents | No such attach report yet |

Based on the table above,that shows why the proposed project using SHA (Secure Hash Algorithm). SHA is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. The SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. SHA256 is a hashing function, not an encryption function. Then, since SHA256 is not an encryption function, it cannot be decrypted. In that case, SHA256 cannot be reversed because it's a one-way function.

SHA256 verification works by computing it again and comparing the result with the result at hand. If both results match, then the verification is successful. The theoretical background is that it's difficult to find another input, which gives the same hash result.

### *D. EXISTING DIGITAL LOCKER SYSTEM*

#### *I) Programmable Digital Electronic Lock*

An electronic lock for use with lockers assigned for transitory or permanent use has a keypad for entering a preselected sequence of digits. Programmable for each use in the transitory mode. The lock shifts a latch to the locked position on a first entry of a sequence chosen by the user, and retracts the latch to unlocked position when the user reenters the same sequence. A subsequent user of the locker when unlocked, can enter any sequence of digits desired. In this mode, the selected sequence is used only to unlock, with the latch or mortise being spring-biased. The construction of the electronic lock is modular, easily fitting on nearly all contemporary locker designs, retained by only a few screws. An outer housing on the outside of the locker door has an electrical plug-in connection through the door with an inner housing on the inside of the door, and the housing portions can be changed to opposite hand use [4]. Power input ports preferably are included on the front of the outer housing to power lock in the event of battery failure. In additional, an audible beep occurs when batteries are low. An

LED indicator can be included for status, as can an infrared reader for instant reprogramming of a large bank of lockers such in a school [5].

### *II) Central Locker System For Shopping Mall Using NFC Based Smartphone*

Depositing purchased item at each store's locker system and carrying a token in hand for the assigned locker while entering a store in a shopping mall as well as collecting the item back while exiting the store is a time consuming exercise and even longer delayed if the token is lost. The time would even multiply visiting multiple numbers of stores in a mall. Sometimes waiting a long queue for depositing item in the store is an irritating hassle and everyone wants to skip this hassle. This paper introduces a novel solution using NFC enabled Smartphone and NFC reader located at each checkout counter of the store which provides an easy and convenient way to immediately keep your purchased things safe at the centrally located locker system and move around openly [6]. Locker number would be generated at the store checkout counter after purchasing the item and just a tap of the smartphone on NFC reader save the locker number information on NFC application installed on a smartphone, which is used to retrieve the item back while exiting the mall [7]. With the proposed solution, usage of extra space for each store's locker system and the corresponding staff can be eliminated, leading to cost reduction, promote efficiency and enhance customer service experience [8].

## III. METHODOLOGY

### *A. System structure*

System structure describes on the workflow of the Double Authentication Locking System using NFC Technology and Password. The figure shown an activity diagram of the workflow for purpose project. In addition, the next Figure shown is a use case diagram that referred as a behaviour diagrams. The use case diagram describes interaction between user and system that shows the relationship user and actions that user involved it. Furthermore, this diagram was identified different types of users of purpose project and different action based on the functional system.

i) Block diagram

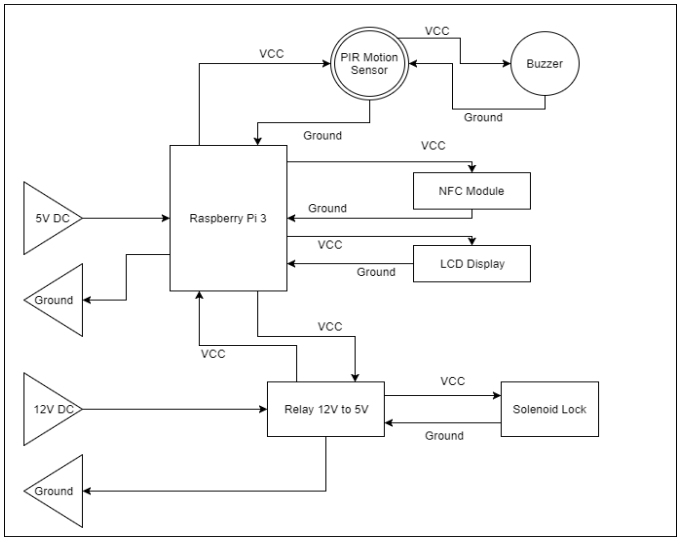


Figure 1 : Block Diagram connection between authentication and system

ii) Use case diagram

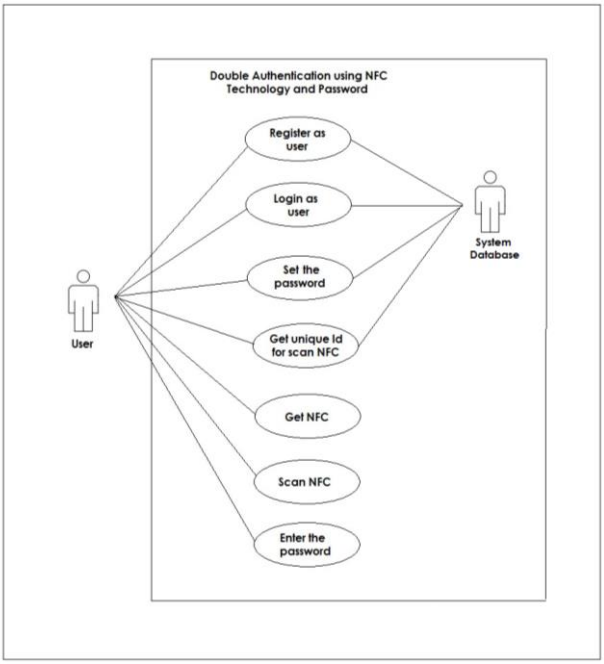


Figure 2 : Use Case Diagram the purpose project

iii) Flow chart diagram

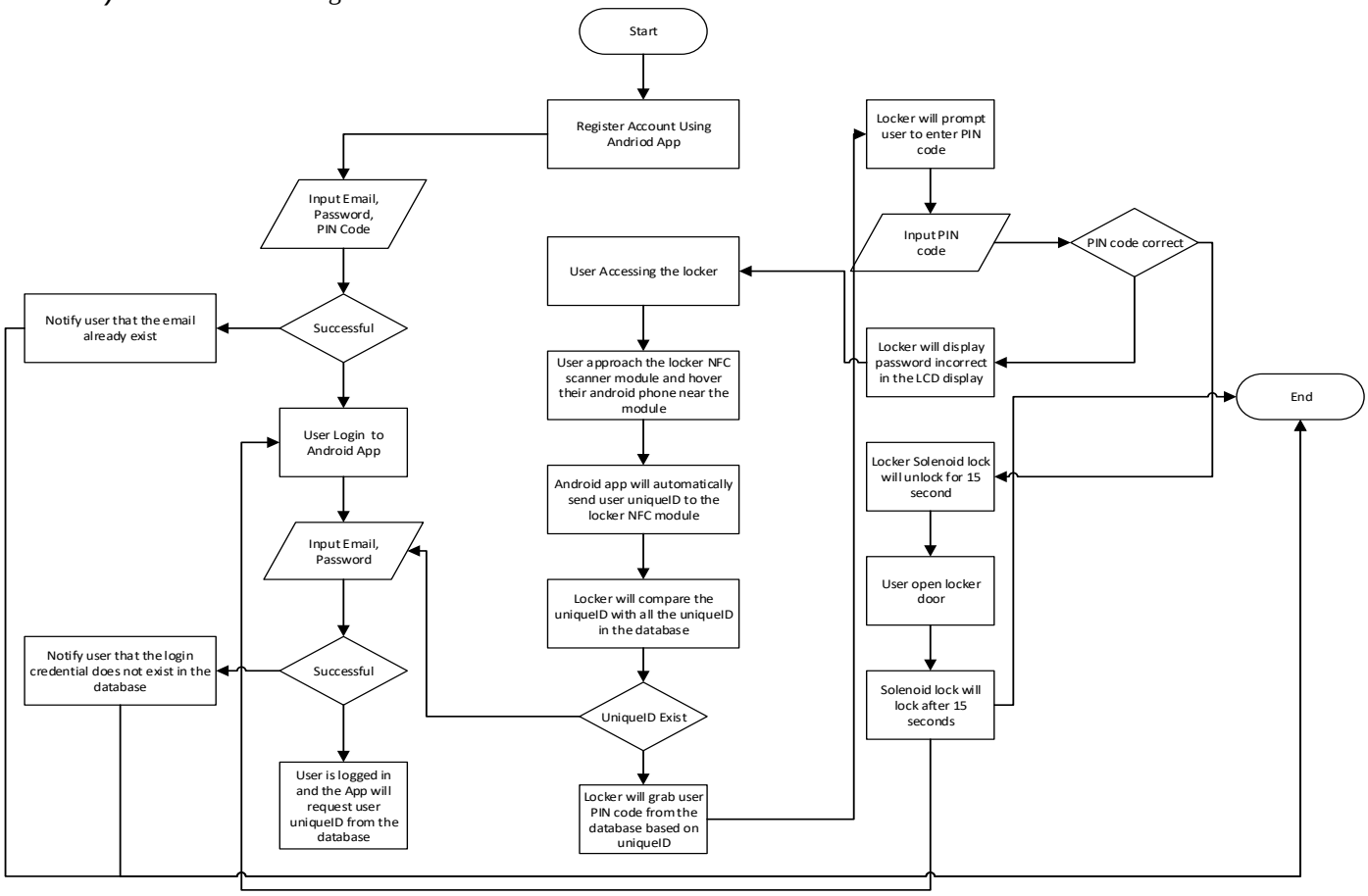


Figure 3 : Flow Chart Diagram the purpose project

## *B. Result and Discussion*

Table 3 : Comparison of Features between Existing Products with the Proposed Project

| | PROGRAMMABLE DIGITAL ELECTRONIC LOCK | CENTRAL LOCKER SYSTEMFOR SHOPPING MALL USING NFC BASED SMARTPHONE | PROPOSED METHOD: DOUBLE AUTHENTICATION LOCKING SYSTEM USING NFC TECHNOLOGY & PASSWORD |
|---|---|---|---|
| COMPANY | Security People, Inc | System LSI Group, Samsung R&D Institute | AFIQAH LIYANA BINTI MOHD JALILI |
| CITATION | Keskin, Y. K., Gokcebay, A. T., & People, I. S. (1997, April 10) | Poddar, S. (n.d.). 25rd October, 2014 | - |
| SMART LOCK | ✓ | ✓ | ✓ |
| APPLICATION MONITORING USING ANDROID SMARTPHONE | - | ✓ | ✓ |
| AUTHENTICATION | PASSWORD | NFC TECHNOLOGY | NFC TECHNOLOGY & PASSWORD |

There are several ways that can be done in order in testing this system. Testing is done in order to know the system reliability, functionality as well as the system usability. It is basically to make sure that the system meets the requirements stated before on the objective. Testing can help in improving the system development for the future, so that any enhancement can be done in any vulnerability found.

There are two types of testing involve for this system. They are:

- Functionality testing
- Security testing

i) Functionality Testing

Functionality testing is a testing technique that is used to test the features or functionality of the system. It should cover all scenarios, including failure paths as well as boundary cases. The system is being tested by providing input and then the results are examining that need to conform to the intended functionality. This testing is conducted on a complete and integrated system to evaluate the system compliance with its requirements.

Several tests have been done to conduct this functional testing for recognition and encryption password authentication. The results of this functional testing are shown below:

Table 4 : Functional Testing

| No. Test | Test cases | Description | Expected results | Actual results |
|---|---|---|---|---|
| Tnp_01 | Test functionality hardware | The hardware can respond NFC device | The LED red light is blinking when the hardware is detected the NFC device | PASSED |
| Tnp_02 | Test authentication 1: NFC technology | Test NFC connection to the hardware | The hardware responds the NFC connection. LED light red are open | PASSED |
| Tnp_03 | Test authentication 2: password | Insert the character password in the text field | The character appears in the text field | PASSED |

### *C. Security Testing*

Security testing is a testing technique to determine if an information system protects data and maintains functionality as intended. It also aims at these six basic principles which are confidentiality, integrity, authentication, authorization, availability and non-repudiation.

Table 5 : Security Testing

| | |
|---|---|
| Description | **Unauthorized user NFC** |
| Steps | 1. Not registered, their NFC can't use the locker |
| Expected result | Access denied when unauthorized user |
| Final result | Pass |
| Description | **Detect the movement of intruders and alarm will ring** |
| Steps<br>Expected result | 1. Intruders try to open the closed locker<br>Alarm will ring |
| Final result | Pass |
| Description | **Guessing the username and password on the login page** |
| Steps | 1. Guess the username and password.<br>2. Scan NFC |
| Expected result | Access denied when inserts the wrong username and password |
| Final result | Pass |

## IV. FUTURE RECOMMENDATION

Several improvements can be added in this project for future development. Due to several weaknesses in this project, some modification and additional elements must include to make sure it improves. So, these are several recommendations to ensure the enhancement of the project can be done:

- Improvise the numpad to biometric technology for more secure.
- The system can be enhanced by adding a function that allows more than one locker to connect to one system.

## REFERENCES

[1] Poddar, S. (2014). Central Locker System for shopping mall using NFC Based Smartphone. Transactions on Networks and Communications, 2(5).

[2] NearFieldCommunication. Security concerns with NFC technology. Retrieved March 24, 2016, from http://www.nearfieldcommunication.org/nfc-security.html

[3] Nield, D. (2016, 06). What is Bluetooth?. *techradar*. Retrieved 12, 2016, from http://www.techradar.com/how-to/computing/what-is-bluetooth-- 1323284 Manjunath, M., Kumar, P., Kumar, P., Gopinath, N., & Haripriya, M. (2015).

[4] Whitehead, J. (1985). Programmable combination lock.Electronic Systems News, 1985(3), 25. doi:10.1049/esn.1985.0075

[5] NFC Based Bank Locker System. *International Journal of Engineering Trends and Technology*,*23*(1), 15-19. doi:10.14445/22315381/ijett-v23p204

[6] Rouse, M. (2015, 06). Authentication. techtarget. Retrieved 03, 2016, from http://searchsecurity.techtarget.com/definition/authentication

[7] Seewoonauth, K., Rukzio, E., Hardy, R., & Holleis, P. (2009). Two NFC interaction techniques for quickly exchanging pictures between a mobile phone and a computer. In *MobileHCI '09: Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services.* (pp. 1-4). New York, NY, USA: ACM. 10.1145/1613858.1613909, Retrieved February 23, 2016.

[8] Statista (2016, 12). Global mobile OS market share in sales to end users from 1st quarter 2009 to 1st quarter 2016. Statista. Retrieved 12, 2016, from https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/