Automatic Lock System for Computer using Bluetooth and Fingerprint Authentication

Wan Hazimah binti Wan Ismail
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
wanhazimah@unikl.edu.my

Ahmad Amirul Afiq bin Abdul Aziz
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
amirulafiq1192@gmail.com

Herny Ramadhani Mohd Husny
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
herny@unikl.edu.my

Norhaiza Ya Abdullah
Malaysian Institute of Information Technology
Universiti Kuala Lumpur, Malaysia
norhaizaya@unikl.edu.my

***Abstract*— Windows Operating System (OS) do have their own authentication policies that provide security to the system. However, these policies do not entirely protect the system from unauthorized user. This is because text-based, password can be easily cracked or stolen by someone else using methods such as brute- force and shoulder surfing. Hence it does not guarantee the safety of the system. This project will focus on developing an automatic locking system for a computer using Bluetooth technology with the fingerprint authentication method. Bluetooth is an open standard specification for a radio frequency (RF) - based, short range wireless technology that is designed to be an inexpensive. Bluetooth technology is suitable for our project because its medium range of communication. To increase the security of our system, we enhance our project by adding fingerprint authentication method. By adding this method, the system only be able to unlock by someone that have registered fingerprint.**

Keywords—component; security; automatic system; computer; Bluetooth; fingerprint; authentication

I. INTRODUCTION

A computer may contain a sensitive work or information that we want to hide from other people. It is important to make sure our computer stays locked when we are not around. Windows Operating System (OS) does have their own authentication policies that provide security to the system. However, these policies do not entirely protect the system from unauthorized user because the security mechanism of Windows does not have a feature to check whether the person logging into the system is indeed the real user or someone who pretend to be the user [1]. This is because text-based, password can be easily cracked or stolen by someone else using methods such as brute-force and shoulder surfing. Hence it does not guarantee the safety of the system. This project will focus on developing an automatic locking system for a computer using Bluetooth technology with the fingerprint authentication method.

Bluetooth is an open standard specification for a radio frequency (RF) - based, short range wireless technology that is designed to be an inexpensive. Bluetooth technology is suitable for our project because its medium range of communication. Not only this is important for the device detection, but also provide a security for the data transmission. The medium range of communication of Bluetooth means that hackers need to be close in order to listen to it communication. There is also a feature called pairing in Bluetooth that allowed only recognized device to make communication with each other. This feature is what we will used before our devices can connect and communicate with each other.

To increase the security of our system, we enhance our project by adding fingerprint authentication method. This method will allow only the real user to unlock the system. We add this authentication method because if the system is able to unlock by Bluetooth detection only, then if someone in possession of user's smartphone, he/she can unlock the system. By adding this method, the system only be able to unlock by someone that have registered fingerprint.

Currently, the old ways of locking the computer by using a timer or manually click on the virtual or physical button on the computer. Then in order to unlock the system, the user needs to key in the correct password or pin number. Even though the system can be locked and unlock using text-based password, the password itself can be stolen. A method like brute force and shoulder surfing can be used by a person that attempt to steal the password. Maybe having a longer password will help to increase the security of the password from being cracked, but the longer the password, the more difficult to remember the password.

For these reasons, we proposed this project to solve the issue with the password. Not only this project can ensure that the system will lock by itself when the user is away, but to make sure only the real user can unlock the system. The main objective of this project can be summarized as follows:

- To study on the current application of computer system authentication using Bluetooth technology.
- To develop the computer system authentication using Bluetooth and fingerprint.
- To test the functionality of the application to lock the computer system.

II. METHODOLOGY

This section summarizes the literature related to this research. It starts with the concept of authentication that links the Bluetooth technology with the biometric authentication that we choose to implement in our system, that is a fingerprint.

A. Authentication

Authentication is the process of validating the identity of someone or something. When a user claims a certain identity, such as by inserting a card into an Automated teller machine (ATM) then typing in a PIN, authentication will decide whether the claim is correct [2]. Generally, authentication requires the presentation of credentials or items of value to really prove the claim of who you are. After the credentials or item are being presented, the authentication process will compare it with the one in the database to check whether the credentials or item is matched.

However, having an authentication process in a system does not always prove the true identity of a person. This is because a credential such as a password can be shared with another person, legally or illegally. A text-based password or a PIN number can be exposed and whoever have the information can claim the identity of the user to the system.

The fingerprint is the most widely used biometric methods in use today. Biometrics is susceptible to error such as false rejection error and false acceptance error, but its sensitivity can be adjusted to increase its accuracy. Nevertheless, biometric system does provide the strongest authentication to prove a person's identity.

Based on the study of three-factor of authentication, we can conclude that having more than one factor of authentication in a system can increase its security. Thus, in our project, we combine two factors of authentication, possession factor and inherence factor, to increase the effectiveness of authentication in our system and make it more reliable. In the next section, we will discuss about first authentication factor we use in our project, possession factor that is Bluetooth technology.

B. Fingerprint Authentication

Fingerprint recognition has been used as a method of identifying since the nineteenth century. According to The Public Domain Review, the projections and dermal folds were described for the first time in the eighteenth century, by the English botanist Nehemiah Grew. There are many algorithms and techniques for the recognition of fingerprints [3]. In Slough History Online, William James Herschel noticed that the fingerprint forms do not change over time. Although he is the first to experimenting with fingerprint and developed the technique of fingerprinting, he only uses it as an administrative tool. It was Francis Galton and Edward Henry that find the fingerprint can be a tool to catch criminals [4].

The purpose of the fingerprint recognition algorithm is to determine whether the two data come from the same fingerprint or not. It can be classified into two categories based on minutiae points or correlation. The first category involves the alignment of two sets of minutiae points and determines the total number of matches. The success of this technique is due to the accuracy, use in detection of minutiae points and also to the use of the complex matching technique in the matching process [5].

The second category is compared and observed global pattern of ridges, after which it can determine the alignment of the two fingerprints. The major disadvantages of this technique include: nonlinear distortion and the presence of "noise" in the picture.

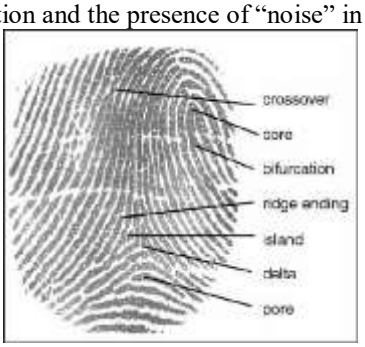

Fig. 1 Example of Human Fingerprint

The image in Fig. 1 above shows example of fingerprint. Ridge endings are the points at which a ridge stops, and bifurcations are the points at which a ridge divides into two. Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other) [6].

C. Bluetooth

J. Haartsen stated that Bluetooth is wireless networks for short range communications that have a widespread usage of Bluetooth radio transmissions between 2400– 2480 MHz by Telecom vendor Ericsson since 1994 [7]. Bluetooth is a low cost component that acts as a connector between two electronic devices that needs to communicate with each other. Bluetooth will provide temporary connection between the two devices. It is a wireless technology developed to replace the cables on devices like mobile phones and personal computers (PC).

This has changed how people use digital devices at home or office, and has changed traditional wired digital devices into wireless devices. According to Yan Ming, and Hao Shi, the normal working area of Bluetooth is within eight meters [8], so it is especially useful in a home or office environment. In Bluetooth, there are several protocols that control different function provides by Bluetooth technology.

D. Comparison of Related Works

We choose several related works that have been done by another author to compare what are differences between their works and ours.

Table 1: Comparison of Related Works

Author	Apoorva Gulhane, Akant Peshin, Pratik Gawand, Bhavik Panchal	Abhishek B L, Anushree Anil Basrur, Divakar P D, Amrutha N K, Rekha K S	Juan-hua, Zhu, Wu Ang, and Guo Kai
Title	Improving Windows Security with Rijndael Encryption and Bluetooth	Bluetooth powered security system	PC lock software design based on removable storage device and dynamic password
Operating system	Windows OS	Windows OS	Windows OS
Description	Windows application system that uses Bluetooth technology to authenticate the user and also secure the users confidential data using Rijndael algorithm.	Windows application that uses Bluetooth technology to lock and unlock computer depends on Bluetooth device availability. Encrypt specific file after system lock.	A software embedded in removable device that lock a computer when it is removed. Encryption key using MD5 algorithm.
Authentication used	Bluetooth authentication	Bluetooth authentication	Removable device
Additional feature	Encrypt file when system lock using Rijndael algorithm	Encrypt file when system lock using DES Encryption	none

From Table 1 above, we can see from the previous works done by another researcher, all of them using just one type of authentication only, that is possession factor. The drawback of using this authentication is that whoever in possession of the device, he/she have the ability to unlock the computer [9]. In our project, we use two types of authentication, which are Bluetooth and biometrics in order to increase the security of the computer. By adding biometric authentication in our project, we can ensure only the real user can unlock the system.

III. DEVELOPMENT

The development of the desktop application is based on Windows operating system while mobile application was based on Android. The hardware needed for this application was a computer running Windows operating system and smartphone that support android operating system. All the programs were being developed by using C# and Java Programming [10]. The details of the development process were discussed in the following section.

A. The Architecture of the System Design

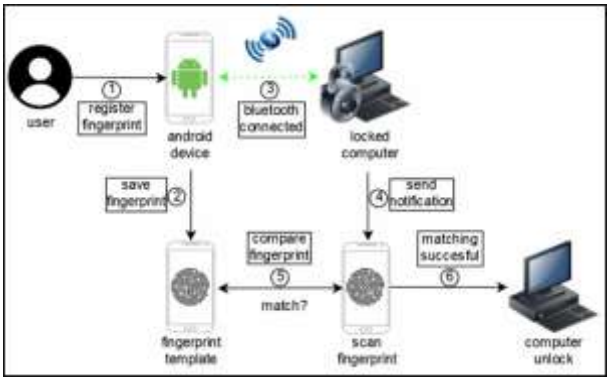

Fig 2: System Architecture Design

This design includes only the important aspects of the system that gives an idea how the system works for the user.

1. Before using the application, users are required to register their fingerprint on android device.
2. The android application will save user fingerprint in their database.
3. When android device comes in computer's Bluetooth range, the android device and computer will connect with each other via Bluetooth. Android device must be paired with a computer first in order for the computer to recognize the device.
4. The computer will send a notification to android device that require user to scan his/her fingerprint. If the android device does not recognize by the computer, it will not receive any notification.
5. The newly scan fingerprint will be compared with the one exist in the android application database.
6. After the fingerprint successfully match, then the computer will unlock.

B. Desktop Application Development

Visual Studio 2017 is used to develop the application. Programming language we used to develop the application is c#. To use this application, a user needs to turn on Bluetooth on the computer. Then the user can open Device setup to pair Bluetooth devices to this computer using this application. After the connection is successful, the user can either use Simple lock or Active lock. Simple lock function to lock the computer manually while Active lock will lock computer automatically. For the unlock, the application will do it automatically. Figure 3 shows the interface of the application.

Fig 3: Desktop Application Interface

C. Mobile Application Development

This application is developed using Android Studio and programming language used is Java. This application can be installed on android version 6.0 and above. When a user opens this application, user first need to pass security authentication. To do that, the user needs to register their fingerprint in smartphone system first before open this application. User can use this application if the authentication is successful. User can change security setting, Bluetooth setting and scan fingerprint using this application. Figure 4 shows the interface of mobile application.

Fig 4: Mobile Application Interface

IV. RESULTS AND FINDINGS

A. Functional Testing

This test is conducted to test functionality of desktop and mobile application that has been developed. Respondent will be given test case for each function of the application as their guideline on how to run the test and what is the expected result from the test. Based on the comparison of expected result with the actual result, respondent will be given each test a pass or fail.

B. Device Setup (Desktop application)

The first test is to test the function of Device setup. The function of Device setup is to list any detected Bluetooth device that in range and link them to this application.

Before this test conducted, the respondent has to make sure the Bluetooth is enabled on the computer and smartphone. For test case 01, when respondent click "Device Setup", a box will appear and show a list of detected Bluetooth device. For test case 02, if respondent chose a Bluetooth device and click "Link this device", the application will connect the device with the computer and show the selected device name. This test to show that the application should be able to connect a smartphone with the computer using Bluetooth.

C. Simple Lock (Desktop application)

This test is to test a function called Simple lock that lock the computer manually. When user click on 'Simple lock', the computer will lock the system and its peripheral device.

In test case 03, before respondent can run the test, they have to make sure their smartphone is connected to the computer. If the precondition meets, the respondent can click "Simple lock" button and then the application should ask for user confirmation to lock the system.

In test case 04, after respondent click yes, when application asking for confirmation, the respondent can turn off Bluetooth on smartphone to test if the application will stays lock the computer. If respondent wants to unlock the computer, the respondent can turn on Bluetooth back. This test to show the application should be able to lock the computer manually and unlock the computer automatically when paired device is detected.

D. Active lock (Desktop application)

Different from Simple lock, Active lock function as the automatic lock when the Bluetooth connection between computer and paired device is lost. From test case 05, the precondition is same as test case 03 where respondent needs to make sure their smartphone is connected to the computer.

After that, the respondent can click "Active lock" button. To test if the Active Lock is functional, the respondent can turn off Bluetooth on their smartphone. The application should automatically lock the computer with its peripheral devices. To test the unlock function, respondent need to turn Bluetooth on and the computer should unlock it.

E. Fingerprint Unlock (Desktop application)

This test is to test for unlocking function that using fingerprint. Different from unlocking function before this that only using Bluetooth, this function required user fingerprint to unlock the computer. When Bluetooth is connected, before computer automatically unlock, the smartphone will receive a notification that required a user to scan their fingerprint on mobile application to unlock the computer.

When the computer is locked, if respondent smartphone is in computer's Bluetooth range, the smartphone will receive notification that requires user to scan their fingerprint on mobile application to unlock the computer.

F. Application Authentication (Mobile application)

This test conducted on mobile application to test its functionality. The first test is to test the authentication of the application.

Before this test conducted, respondent needs to register their fingerprint in the system. When respondent opens the application, they required to pass fingerprint authentication before can use the application. This is to prevent from anyone other than registered user can use this application.

G. Setting (Mobile application)

This test is to test if user able to open security and Bluetooth setting in the mobile application. Setting button is used if the user wants to change security or Bluetooth setting of the smartphone.

After respondent can access the application, theyshould see these buttons on Home interface. When respondent click these buttons, the mobile application should bring them to their respective setting on a smartphone.

H. Fingerprint Authentication (Mobile application)

The last test is to test if the user can use fingerprint authentication to unlock the computer. When Bluetooth is connected, before computer automatically unlock, the smartphone will receive a notification that required a user to scan their fingerprint on mobile application to unlock the computer.

Table 2: Summary of functional testing result

Test id	Description	Expected result	Actual result	Pass/fail
01	Precondition: Bluetooth is enable on computer and smartphone. User click "Device Setup" button.	"Device setup" box will appear and show list of detected Bluetooth devices.	As expected.	Pass.
02	Precondition: User smartphone Bluetooth is in list of devices. User choose his/her smartphone Bluetooth and click "Link this device" button.	A box will pop up and notify user the connected device name.	As expected.	Pass.
03	Precondition: User smartphone connected to the computer. User click "Simple lock" button.	A box will pop up to ask user for confirmation to lock the system. After user click yes, the system will lock.	As expected.	Pass.
04	Precondition: User click yes after confirmation box pop up when user choose "Simple lock" button. Off Bluetooth on user smartphone. On Bluetooth on user smartphone.	When Bluetooth is off, system stays lock. When Bluetooth is on, system will unlock.	As expected.	Pass.
05	Precondition: User smartphone connected to the computer. User click "Active lock" button. Off Bluetooth on user smartphone. On Bluetooth on user smartphone.	When Bluetooth is off, system automatically lock. When Bluetooth is on, system automatically unlock.	As expected	Pass
06	Precondition: System is lock. User attempt to unlock system using fingerprint authentication on android.	User smartphone receive notification to unlock system using fingerprint.	As expected.	Pass.
07	Precondition: User register fingerprint on device. User open application. User need to pass fingerprint authentication to use application.	User with registered fingerprint has permission to use the application. User with no registered fingerprint will denied access.	As expected.	Pass.
08	Precondition: user can access the application. User click "Security setting".	Application will show security setting of the phone.	As expected.	Pass.

09	Precondition: user can access the application. User click "Setup Bluetooth"	Application will show Bluetooth setting of the phone.	As expected.	Pass.
10	Precondition: user can access the application. When user smartphone in computer's Bluetooth range, smartphone will receive notification that ask user to scan fingerprint to unlock computer.	If success, the computer will unlock.	Integration part is not complete.	Fail.

CONCLUSION

As conclusion, we have successfully done our research on the current application of computer system authentication using Bluetooth technology. Based on the research we have done, we found that Bluetooth technology is suitable to be implemented into our project. Feature like service discovery protocol is crucial in our system.

We also manage to develop a desktop application that capable to lock the computer system by using the Bluetooth connection. The develop system manage to fulfil some of the objectives of this project that is to develop a computer system authentication using Bluetooth.

After the development of the application, we proceed to test the functionality of the application to lock the computer. The result, we get from testing our current application is not like we expected because some part of the application is not yet finish. We can get a better result if the development of our application is complete. Nevertheless, this application still can help user to automatically lock the computer when the user is away from the computer. Therefore, there is no need for user to manually on/off the computer every time user go away from the computer or come back to the computer.

REFERENCES

[1] Abhishek, B., Basrur, A. A., Divakar, P., Amrutha, N., & Rekha, K. (n.d.). BLUETOOTH POWERED SECURITY SYSTEM. 2016.

[2] Rasmussen, K. B., Roeschlin, M., Martinovic, I., & Tsudik, G. (2014). Authentication Using Pulse− Response Biometrics. Presented at the The Network and Distributed System Security Symposium (NDSS).

[3] Leelambika, K., & Rohini, A. (2013). Bayes Classification for the Fingerprint Retrieval. International Journal of Advanced Research in Computer Science, 4(2).

[4] Dakhil, N. K., Mohamed, H. R., & Mohsin, N. A. (2013). Fingerprint Recognition using extraction of connected boundaries components edge detection.

[5] Kim, W. (2013). A multistage fingerprint recognition method for payment verificationsystem. International Journal of Security and Its Applications, (2), 335–365.

[6] Tewari, K., & Kalakoti, R. L. (2014). Fingerprint recognition using transform domain techniques (pp. 136–140). Presented at the Proceedings of the International Technological Conference.

[7] Haartsen, J. (1998). Bluetooth-The universal radio interface for ad hoc, wireless connectivity. Ericsson Review, 3(1), 110–117.

[8] Karnan, M., & Krishnaraj, N. (2010). Bio password—keystroke dynamic approach to secure mobile devices (pp. 1–4). Presented at the Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on, IEEE.

[9] Singh, S. P., Ayub, S., & Saini, J. (2016). Literature survey on different type of fingerprint recognition (pp. 3748–3755). Presented at the Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on, IEEE.

[10] Juan-hua, Z., Ang, W., & Kai, G. (2010). PC lock software design based on removable storage device and dynamic password (Vol. 3, pp. V3-326). Presented at the Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, IEEE.