Seamless Personnel Authentication using Facial Recognition and Identity-Based Identification on Mobile Devices

Jun-Ren Tan, Wai-Kit Chin, Ji-Jian Chin and Vik-Tor Goh

Abstract*: Security systems for buildings are no longer an uncommon thing in daily life with increasingly complex access control systems to achieve secured building security system. Achieving a hassle-free yet secure access control systems has been always a challenge for organizations especially for those managing large buildings. In this project, we develop a prototype that utilizes a combination of biometric and cryptography based security schemes to grant access control on personnel going in and out of a building. Our development achieves two-factor authentication in one single step which provides users a seamless experience for authentication. The identity-based identification (IBI) scheme that is based on number-theoretic cryptography is implemented on mobile devices to allow the identification scheme to run in the background. A face recognition system and web server is also developed which can be deployed on any PC at the market. The novelty lies in the combination of the two, with the face recognition making potential intruders difficult to forge biometric data of honest users, and the identity-based scheme preventing the adversary to learn any secrets from the authentication process, while allowing honest users to verify themselves from face to smartphone without any user intervention, thus creating a seamless authentication experience.

***Index Terms*: Face Recognition, Identity-based Identification, Mobile Application, Door Lock, Seamless Two-Factor Authentication.**

I. INTRODUCTION

Building access control system is widely used in this technological era. Usually the handling access control of large organization requires new visitor to register at reception area and receive a pass for the entrance. Most of the existing commercialized smart building security systems have many drawbacks in the way that NFC, RFID-based and even smartphone-based schemes can either lost, cloned, or misused by irresponsible individuals. The limitations of existing systems also require some form of human intervention which may cause some inconvenience especially to the elderly and disabled who try to perform authentication. While the conventional method is still be applicable, it does not utilize the technology that is available effectively. In pace with advancement of technology, smartphones have become an essential part of human's life. In accordance with a research in Pew Research Center, three-quarters of adults own a smartphone [5]. 88% of the smartphones are android and 11.9% are iOS platform according to The Statistics Portal with statistic and studies from more than 22,500 sources [6].

In this paper, we present a prototype that utilizes the background authentication process for the access control system using Android or iOS application in combination with a face recognition system. Powered by a number-theoretically secure Identity-Based Identification (IBI) scheme in combination with a biometric-based face recognition system, our prototype achieves two-factor authentication in one single step. This provides users a better experience instead of adding troublesome steps and at the same time provide a highly secured but less disruptive smart building access control system.

A. *Motivations*

This work is motivated by the apparent widespread and ease of development for smartphones as well as biometric-based identification schemes available. By combining the two, we are able to remove the disadvantages that current card-based systems suffer from. Below are the potential benefits of our work to enhance building access control system:

1) Reduce the use of ordinary keys, tags, pass, and security personnel hired which will result in saving cost for large organizations.
2) Since our prototype require face recognition to perform identity-based identification, it is able to prevent someone else to counterfeit an identity or steal and miss use provided tags or smartphone as the key to enter the a building. Only a person's face face can be used in conjunction with his/her smartphone to access the site.
3) Compared to the previous work by Teh et al. 2015 [4], our system is able to prevent the door from being unlocked by mistake when the users are not in front of the door, for example when users click unlock button in the smartphone application in anywhere of the building.
4) Since the authentication is performed in the background automatically, entering the site has made less disruptive and no human intervention is needed, making the authentication process more convenient to people especially for the elderly and disabled.

Revised Manuscript Received on August 18, 2019.

Jun-Ren Tan, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.
Wai-Kit Chin, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.
Ji-Jian Chin, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.
Vik-Tor Goh, Faculty of Engineering, Multimedia University, Cyberjaya, Malaysia.

5) Our prototype logs details of all authentications that are trying to unlock the door which allows the system to track any unauthorized users that are trying to access the site. This could ease the both forensics and supervision of any suspicious activities.

6) Registration for visiting the site is also convenient. Anyone with the mobile application can now register themselves to the access control system while administrators can remotely authorize these registrations to grant users access.

7) Administrators also have the authority to blacklist any personnel by de-authorizing the users in the system. This could reduce the amount of unwanted and wasted tags or cards.

B. *Related Work*

As far as our knowledge goes, there is no other work in literature combining both biometric-based face recognition identification and IBI schemes. IBI schemes implemented on the mobile device allows the mobile device to act as prover to prove its identity to the verifier without giving away any information of the secret it holds. Face recognition identification limits that only faces registered in the system can proceed to perform the specific IBI protocol. Prevoius work by Teh et al 2015[4] successfully developed a prototype with IBI protocol on smart phones. Our work is seen as an extension to that work to enhance the prototype with the implementation of face recognition to achieve higher security and seamless authentication process.

While there are work using either smartphone or face recognition to gain door access, including door lock control systems based on NFC smartphones developed by Hung, C. H et al. 2015 [3], they do not describe the cryptographic algorithm they used to secure the system from adversaries, whereas the face recognition system based on auto-switching magnetic door lock system using microcontroller by Hassan et al 2012 [2] do not implement cryptographic schemes behind it. Both these prototype do not achieve two-factor authentication and user-friendly registration.

There are also some existing commercialized smartphone door lock system including Yale Assure, Schlage Sense, August, Kwikset Kevo. However, these system also do not advertise the security algorithm they implemented to secure the system which leaves their security capability questionable. As far as we know, no working prototype implement both IBI and biometric-based recognition to achieve dual factor authentication in a single step.

C. *Contributions*

Our work is an extension from the previous work of providing access control using an IBI scheme on mobile smart devices [4]. However, Teh et al.'s 2015 [4] prototype developed a mobile application with GUI that still requires a user to tap the button in application to perform authentication manually. Our prototype enhances this by pushing the IBI scheme to the background and complements the protocol by face recognition initiation to achieve a seamless user experience. Our developed prototype also achieves dual-factor authentication in just one simple step. At first, our developed prototype utilizes the face recognition system to recognize the identity of users who try to enter the building through a security camera's video feed. Once the subject passes the face recognition identification, the user's mobile device will receive push notification. Upon receipt of the notification, the mobile application will then perform the IBI protocol for the door lock with the respective server based on the payload of notification.

The advantages of the system is such that after a user passes the face recognition, every process from server from push notification until unlocking the door will be run in the background without any human intervention needed.

To perform face recognition and authentication process, user's face and his mobile device has to be registered to the server through application registration by themselves or web registration perform by admin or receptionist. Every mobile device will be identified uniquely by their Gmail account's email address. Our prototype server runs on a local network pc which can only be accessed by mobile devices through the same local network WiFi. The benefits of putting the server in a local area network rather than the internet is that it could prevent any potential adversarial attack through the internet. Thus, the authentication could only perform by the mobile device which is connected to the local Wifi.

A distributive software environment is created such that the whole system and server can be distributed on any computer easily. Our prototype is able to deploy at any organization that require access control system such as office buildings, hotels, government institutes and apartments.

II. OVERVIEW.

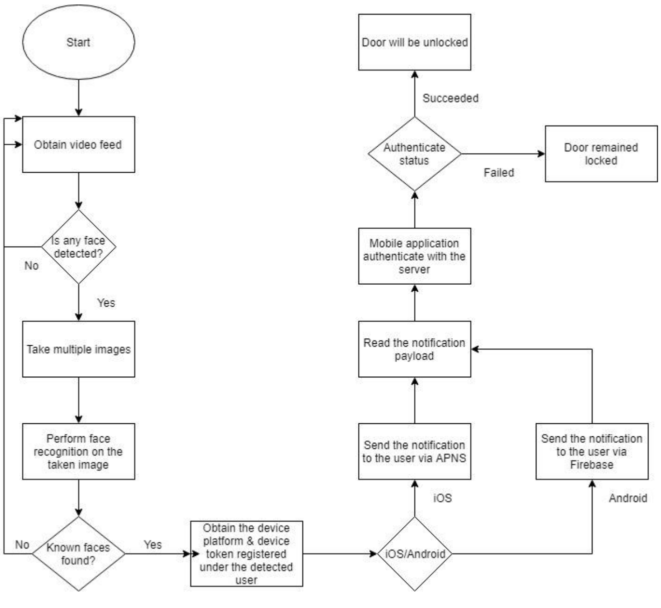

Start
Obtain video feed
Is any face detected?
No
Yes
Take multiple images
Perform face recognition on the taken image
No
Known faces found?
Yes
Obtain the device platform & device token registered under the detected user
iOS/Android
iOS
Android
Send the notification to the user via APNS
Send the notification to the user via Firebase
Read the notification payload
Mobile application authenticate with the server
Authenticate status
Failed
Door remained locked
Succeeded
Door will be unlocked

Fig. 1. Overall Process

Figure 1 shows the complete process of the prototype to unlock the door lock. First, the facial recognition will obtain video feed from CCTV, if any faces are detected in the video feed, it will take multiple images of the face and perform facial recognition on the taken images. If the face is known in the database, it will create a text file with the detected users name with it. A python script is responsible for obtaining the device platform and act accordingly on the user's device platform. Next, a push notification will be sent via APNS or Firebase according to the device platform. After sending the notification, the mobile device will read the notification payload and trigger the background authenticate process without interaction needed between users and the mobile device.

III. Identity-based Identification Schemes

The IBI scheme used in the prototype was proposed by Kurosawa and Heng[1]. The IBI scheme consists of three phases which are Setup, Extract and Identification.

1) Setup: A random generator g and secret s is selected. Define g_1 to g^s. The generated master public key is generated and published while the generated master secret key $msk = s$ is stored as a secret.

2) Extract: Each user must register to the registration server with an identity-string and the identity-string is used as the user's public key. The user secret key (usk) is then generated and stored in the user's device.

$$Q = H(ID)\#(1)$$
$$usk = D = Q^s\#(2)$$

3) Identification: The protocol is executed between the prover and the verifier when the prover wants to prove its identity to the verifier.

   a) Prover sends a commitment to the verifier by generate a random, r then compute $U = Q^r$ and send U to the verifier
   b) The verifier sends a random generated challenge, c to the prover
   c) Prover generates a response $V = D^{r+c}$ and send it to the verifier.
   d) Verifier accept if $e(g, V) = e(g_1, UQ^C)$.

The correctness can be checked using the equation:

$$\begin{aligned} e(g, V) &= e(g, D^{r+c})\#(3) \\ &= e\left(g, Q^{s(r+c)}\right)\#(4) \\ &= e(g^s, Q^r Q^c)\#(5) \\ &= e(g_1, UQ^C)\#(6) \end{aligned}$$

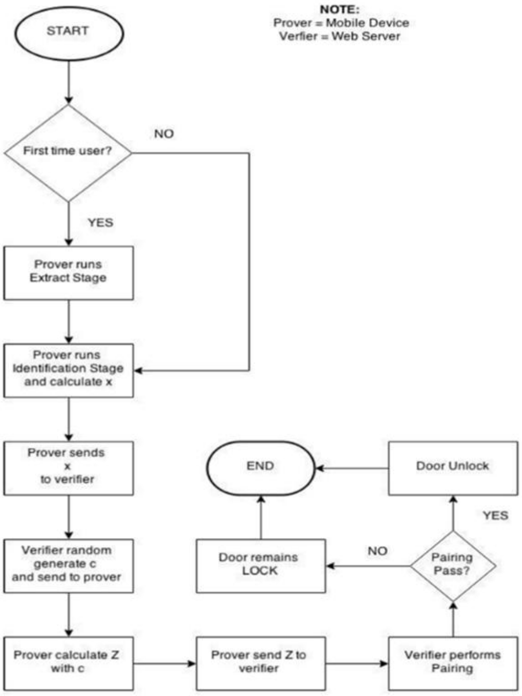

NOTE:
Prover = Mobile Device
Verfier = Web Server
START
First time user?
NO
YES
Prover runs Extract Stage
Prover runs Identification Stage and calculate x
Prover sends x to verifier
Verifier random generate c and send to prover
Prover calculate Z with c
Prover send Z to verifier
Verifier performs Pairing
Pairing Pass?
YES
NO
Door Unlock
Door remains LOCK
END

Fig. 2. IBI on mobile device flowchart

Figure 2 shows the flow of Identity-Based Identification that is implemented on mobile devices.

IV. METHODOLOGY

A. *Server*

XAMP server is used to establish the server-client architecture. The server can only be run in the local network such that no one can access the building security system without physically present in the building. The communication between the mobile device is done through the PHP web pages which act as a communication bridge between the mobile device and database. The communication process is illustrated in Figure 3 shown below.

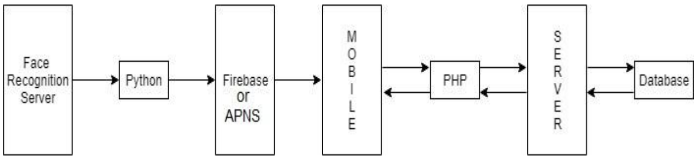
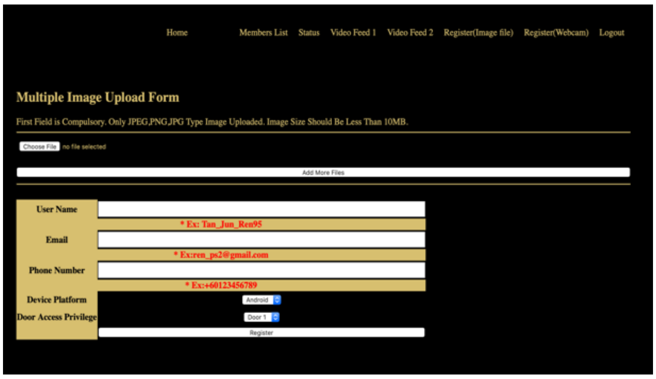


Fig. 3. Communication Process.

After a user passes the face recognition, starting from the python script to server until the door is unlocked, every communication process will be run in the background without any user interaction needed. Firebase and APNS are used in this project to send push notification to the mobile device. The face of a user will become the key to the door and the mobile device will act as the ID for the user. The mobile device is used to become the prover of authentication stage in IBI security algorithm.

The pairing library for the IBI scheme is written in Java and exported as JAR file. The JAR file is invoked by the PHP through the Java Bridge. Administrator's pages are created to allow the administrator to perform various task such as registration, the user information and authorize or de-authorize any users.



Multiple Image Upload Form

First Field is Compulsory. Only JPEG,PNG,JPG Type Image Uploaded. Image Size Should Be Less Than 10MB.

no file selected

User Name
* Ex: Tan_Jun_Ren95

Email
* Ex:ren_ps2@gmail.com

Phone Number
* Ex:+60123456789

Device Platform: Android

Door Access Privilege: Door 1

Fig. 4. Administrator Registration Page.

B. *Face Recognition*

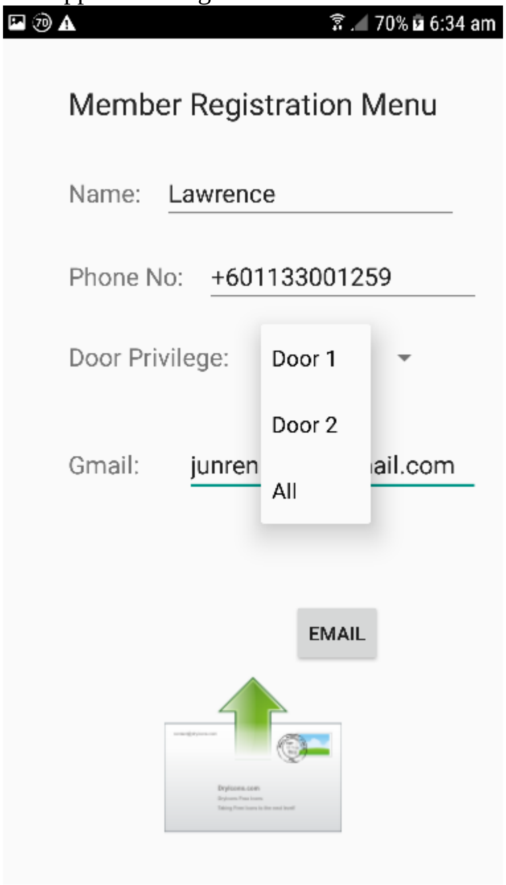
The Dlib library is used for facial recognition. Before face recognition can be performed, the user must provide their own photos to the face recognition system. This can be done via the developed web portal and mobile application. The face in each photo is then encoded and stored inside the KNN(K-Nearest Neighbor) classifier. The developed face recognition takes in input from multiples video source. If the system is able to detect any face from the video source, it will convert the video frames which contain human face to image before face recognition is performed. The image is then loaded to the face recognition system and the detected face is then compared with the face encoding stored in the KNN classifier. The identity of the user is identified if the user face encoding is similar to the face encoding stored in the KNN classifier. Once the user identity is identified, the log of the face recognition system will be updated.

The face recognition system will then send a push notification to the user device via Apple Push Notification Service or Firebase using the user device token. The push notification allows the device to perform the authentication without any user interaction.

C. *Google Android Platform*

The development of android application is done using Java programming language and Android Studio IDE. The developed android application allows any users to register their mobile device and face to the server. Data communicate between android application and the server is through PHP. The android application is capable of obtain the details of the mobile devices such as the primary Gmail of the user device. The email will be used as a unique ID for Extract and Identification.

The android application is designed to work without user interaction. Thus, the push notification capability is implemented where it can receive and read the push notification and perform authentication to the relevant server based on the payload of the push notification. Figure 5 shows the android application registration interface.



Member Registration Menu

Name: Lawrence

Phone No: +601133001259

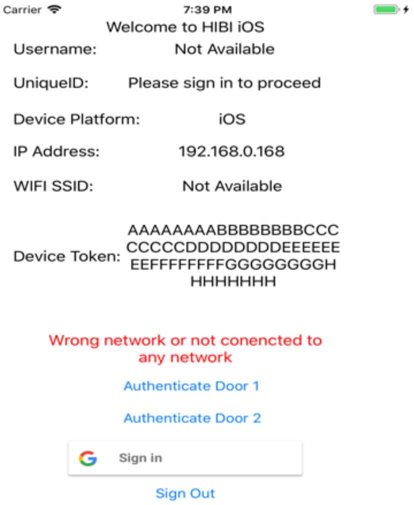
Door Privilege:

Gmail: junren ail.com

Fig. 5. Android Application Registration

D. *Apple iOS Platform*

The development of iOS application requires Swift and Objective-C programming skills. As opposed to the developed Android application, iOS doesn’t allow its application to obtain any unique detail from the user device. Therefore, Google Sign-In API is integrated into the iOS application such that the user can sign in to the Google accounts via the developed application and the signed-in Google account address will be used for the Extract phase. In order to facilitate the user to switch between their Google accounts, the developed application also allows the user to sign out their Google account. Since the application is expected to work without user interaction, the developed iOS application is enabled with push notification capability where it can receive and read the push notification then perform authentication to the corresponding server based on the content of the push notification. The screenshot of the developed application is found in Figure 6.



Welcome to HIBI iOS

Username: Not Available

UniqueID: Please sign in to proceed

Device Platform: iOS

IP Address: 192.168.0.168

WIFI SSID: Not Available

Device Token: AAAAAAAABBBBBBBBCCC CCCCCDDDDDDDDEEEEEE EEFFFFFFFFGGGGGGGGH HHHHHHH

Wrong network or not conencted to any network

Fig. 6. iOS Application

E. *Door Lock System*

The door lock system is setup using Cytrone UNO controller, Bluetooth HC-06 module, logic circuit and a pair of electromagnetic door lock as shown in the Figure 7.

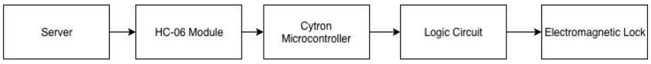


Fig. 7. Block Diagram of Door Lock System.

The server will send a message to the HC-06 Module through a secured Bluetooth serial connection such that the adversary will not able to gain knowledge on the content of message send by the server. The Cytron microcontroller reads the received message and if the message match one of the predefined message, the corresponding electromagnetic door lock will be powered down by shorted the transistor to ground. There are 2 door locks which represent Door 1 and Door 2. The developed door locks are shown in Figure 8.

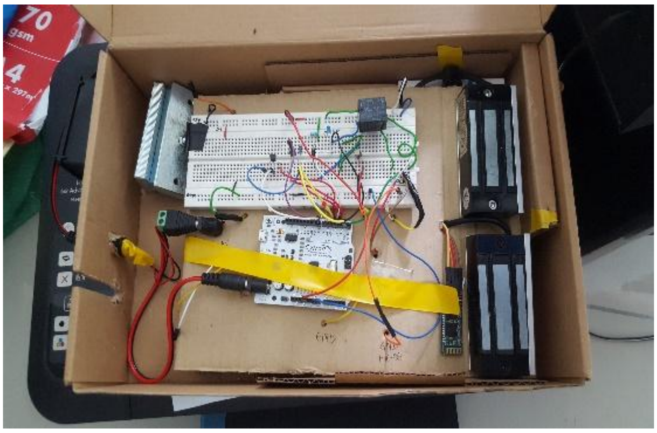


Fig. 8. Door Lock System

V. Prototype Experiment Results and Discussions

We conduct the face recognition performance and Setup stage test using MacBook Pro 2016 which comes with dual-core 2.0GHz Intel Core i5 and 8GB of RAM. Meanwhile, the Extract and Identification experiment is established using Apple IPad mini 2(for iOS application) , Samsung Galaxy S6(for Android application) and MacBook Pro 2016 which acts as the server.

We perform a complete face recognition cycle for 25 times and the average time needed to complete a cycle is computed in the table below. The performance parameters(accuracy rate, false negative rate and error rate) of the developed face recognition system is also evaluated by sampling a population of 25 people.

TABLE I. Average Time Needed To Complete One Face Recognition Cycle

Average time needed(s)
7.8143543

TABLE II. Performance Parameter Of The Face Recognition System

Performance parameter	%
Accuracy Rate	92
False negative rate	4
Error rate	4

The Setup performance test, Extract performance test and Identification performance test are also conducted for 25 times for different platforms and the average time needed to complete it is tabulated in the table below. Last but not least, we also conduct the performance test for 25 times which evaluates the average time needed to complete the authentication while the application is running in the background for different platforms using the same setup mentioned above.

Since there are no other work which implements such as a two-factor authentication system, we benchmark our results against that of Teh et al. 2015 [4] which is the closest comparison. In contrast with their method of executing the JAR using shell execution prompt within PHP, we implemented Javabridge to execute JAR files which is a safer alternative that prevents adversaries from altering the PHP script to perform malicious task. However, this results slower Identification stage for our prototype. We argue that this slight delay is negligible in view of having better hardware available these days to help balance the speed of process.

For the background process authentication it also takes longer time as the developed Android application will be given a lower processing priority when the Android application is running in the background. The delay in developed iOS application is caused by the fact that the iOS will suspend the developed application when the user left the application/screen off and the developed application will have to restart itself once the device receive the pre-defined push notification.

TABLE III. Average Setup Time

Platform	Average Setup time(ms)
MacBook Pro 2016	11.5
Teh et al [4]	181.046242

TABLE IV. Average Extract Time

Platform	Average Extract time(ms)
Android	1182.8
iOS	324.188605
Teh et al [4]	776.576779

TABLE V. Average Identification Time

Platform	Average Identification time(ms)
Android	1132.1
iOS	2276.0855749
Teh et al [4]	814.100231

TABLE VI. Average Time To Complete The Authentication While The Application Is Running In Background

Platform	Average time needed to complete the authentication(s)
Android	11.98458925
iOS	13.016753

VI. Conclusion

The face recognition system can be improved by adding liveness detection by reading the change in microexpressions or any other feasible approach. IBI scheme can be augmented to achieve Hierarchical IBI which allow users to generate a temporary child keys for visitors. Besides that, time restriction feature can be added also to limit a personnel to unlock the door only at 9am-6pm daily or set a 2 hours limit to a visitor. Last but not least, improvements can also be done to speed up the whole authentication cycle and better battery consumption.

ACKNOWLEDGMENT

Financial support from the Ministry of Higher Education, Malaysia, under the Fundamental Research Grant Scheme with grant number FRGS/1/2015/SG07/MMU/02/1 is gratefully acknowledged

REFERENCES

1. K. Kurosawa, & S. H. Heng, “Identity-based identification without random oracles”. In *International Conference on Computational Science and Its Applications*, Springer, Berlin, Heidelberg, pp. 603-613.
2. H. Hassan, R. A. Bakar, & A. T. F. Mokhtar, “Face recognition based on auto-switching magnetic door lock system using microcontroller”. In *2012 International Conference on System Engineering and Technology (ICSET)*, IEEE Xplore, pp. 1-6.

3. C. H. Hung, Y. W. Bai, & J. H. Ren, "Design and implementation of a door lock control based on a near field communication of a smartphone." In *Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference*, IEEE Xplore pp. 45-46.
4. T. Y. Teh, Y. S. Lee, Z. Y. Cheah, & J. J. Chin, "A Prototype to Facilitate Access Control Using Identity-Based Identification on Mobile Smart Devices." In *2015 5th International Conference on IT Convergence and Security (ICITCS), IEEE Xplore* pp. 1-5.
5. Pew Research Center. (2018, February 5). Mobile Fact Sheets. http://www.pewinternet.org/fact-sheet/mobile/
6. The Statistics Portal (2018). Mobile OS Market Share 2018. https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/.

AUTHORS PROFILE

Jun-Ren Tan obtained his Bachelor of Engineering, majoring in Computer Engineering from Multimedia University in 2018. He is now an entrepreneur working with telecommunication services.

Wai-Kit Chin graduated from Multimedia University in 2018 with Bachelor of Engineering, majoring in Computer Engineering. He is currently working on mobile application development at Motorola Solutions

Ji-Jian Chin holds a PhD from Multimedia University and is a senior lecturer at the Faculty of Engineering, Multimedia University. He is currently working on bridging the gap between theoretical and applied cryptography with real-life engineering prototypes.

Vik-Tor Goh received his B.Eng. (Hons.) Electronics and M.Eng.Sc. degrees from Multimedia University, Malaysia. Following that, obtained a PhD in Computer Science from Queensland University of Technology, Australia in 2010 for his research on intrusion detection. He was awarded the (ISC)2 Information Security Scholarship in 2007 and 2008 for his pioneering work in intrusion detection. His current research interests include information security, IR4.0, and IoT. In addition to a being a qualified Professional Engineer (PEng, BEM) and Chartered Engineer (CEng, IET), he is also certified as a CISSP, CCNA, and HCDA.

Retrieval Number: C10091083S19/2019©BEIESP
DOI:10.35940/ijrte.C1009.1083S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication