International Journal of Current Research and Review
DOI: http://dx.doi.org/10.31782/IJCRR.2021.131227

Scopus

Original Research

IJCRR
Section: Healthcare
ISI Impact Factor (2019-20): 1.628
IC Value (2019): 90.81
SJIF (2020) = 7.893

A Fingerprint Authentication for Android-Based Healthcare Appointment Scheduling System

Abdulmalek Al-Shujaa[1], MS Nabi[2], Qusay Al-Maatouk[3], Abdulaleem Zaid Al-Othmani[4], NAA Rahman[5]

[1,2,3,5]School of Computing and Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia; [4]Malaysian Institute of Information Technology (MIIT), Universiti Kuala Lumpur (UniKL), Kuala Lumpur, Malaysia.

ABSTRACT

Introduction: Healthcare organizations maintain patient sensitive data that requires to comply with privacy and security laws. At the same time should provide a system with ease of access.

Objective: The main purpose of this research is to develop a mobile application that can manage, and control patients flow at the healthcare by allowing the doctor to upload their appointments and then allow clients (patients) to book one of the available slots in an efficient and effective way.

Methods: A survey has been conducted on 100 android app users in Malaysia, it has been observed that businesses' owners does not trust current mobile appointment applications and prefer to use the traditional methods, which is on first come, first serve bases. Aside from that, current issues that are faced by the users are that most of the mobile appointment applications are unsecured and there is no security control over the account holders for these applications.

Results: The developed application also includes extra feature such as secure chatting function that links between the users of the app and let them discuss any type of inquiries related to the booked appointment. AES, SHA-256 and SCRYPTE algorithm has been implemented successfully on the developed application and hence will increase the layer of security and keep user data in a safe manner. AES encryption used to encrypt the users chatting messages while the SHA-256 used to hash the secret key that used to encrypt and decrypt data. Moreover,

Conclusion: Biometric fingerprint authentication has integrated with the system in order to solve the existing security flaws of the current appointment applications as well as email verification for avoiding the anonymous user and increase the overall security features.

Key Words: AES, Appointment System, Fingerprint Authentication, Healthcare, SCRYPTE, SHA-256

INTRODUCTION

According to a survey conducted on 100 android app users in Malaysia, it has been observed that most of the businesses' owner does not trust current appointment mobile applications and prefer to use the traditional methodology which is based on "first-come, first-serve". The current issues that are faced by the users are that most of the mobile appointment applications are unsecured and there is no security control over the account holders for these applications. [1] For example, a user can create an account and book an appointment anonymously without any sort of verification being conducted by the application. Aside from that, even after an appointment is booked, still patients usually need to queue at the business enterprise for a long time before getting served. This means the currently available appointment scheduling system is cumbersome, time-consuming, constant manual management and fallible.

Moreover, the currently available apps do not provide high security to end-users. These applications allow users to create an account and book an appointment without any security measurements such as sending a one-time password for confirming the booking process etc. These issues led security technologies such as biometrics authentication, email verification and cryptography to get involved in apps development and help users and business owners to maintain business flow in an effective, efficient and secure manner. The proposed solution for the issues discussed earlier is to develop a secure mobile appointment scheduling app.[2,3]

Corresponding Author:
NAA Rahman, School of Computing and Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia.
E-mail: nor_azlina@apu.edu.my

ISSN: 2231-2196 (Print) **ISSN:** 0975-5241 (Online)

Received: 28.10.2020 **Revised:** 15.12.2020 **Accepted:** 14.02.2021 **Published:** 22.06.2021

Considering scheduling and managing appointments at the healthcare service provider, the proposed app will manage and control the patient's flow by allowing the clinic assistant to upload their business appointments and then allow clients to book one of the available appointments efficiently and securely. In addition, the expected application will have biometric fingerprint authentication to solve the existing security flaws of the current appointment applications as well as implementing a secure channel that links the application's users and the database. The proposed mobile application will have email verification to avoid the anonymous user and increase the layer of security. The development of any system in the healthcare sector requires extra attention to the privacy of the patient's data. Hence, healthcare-related systems should pay more attention to patient's data privacy from the early stages of the system design.[4,5]

Literature Review

One study has studied the fingerprint-based on recognition method and performance analysis.[1] The fingerprint is the common and alterable method that uses intentionally as a legal method to identify a person. Plus, the fingerprint uses in numerous application that uses in the military, law enforcement, medicine, education, civil service, and forensics. The researchers have compared the biometrics technologies based on the EER (Equal Error Rate), FAR (False Acceptance Rate) and FRR (False Rejection Rate). Based on these comparisons, the researchers observed that fingerprint recognition has the strongest biometric authentication amongst the other biometric technologies and agreed that fingerprint recognition is the best biometric technology for explosives security from an analysis of the requirements. A few studies have compared among three types of fingerprint scanners and simplify the process of enrollment, identification and verification.[2,3] The fingerprint recognition consists of four stages which are capturing the biometric data, pre-processing stage, extraction stage, and matching stage [4]. In the enrollment stage, the biometric data is acquired from the sensor and stored in a database along with the person's identity for the recognition process. The biometric data is captured, and the digital image will be created and then pre-processing applies to the digital image to remove unwanted data as well as apply the post-processing. Lastly, the data will be stored on the database and trigger according to the user needs. In addition, the retrieved data will be compared with the user finger pattern with the template in the database. The biometric data is re-acquired from the sensor during the recognition mode which will be compared to the stored data to determine the user identity.

Hashing Algorithms

Password hashing is the most common approach for maintaining users' password-related information that later use to authenticate the user.[5] Therefore, the password of the user will be hashed and store in the database as a hashed value and then when the user logs in the hashed values will be compared and login to the system if the hashed values are matched. Moreover, the authors have reviewed all such algorithm and proved the weakness behind each one.[6] There exist several hashing algorithms and each one has its advantages and limitations. For example, when comparing (Secure Hash Algorithm 1) SHA-1 and (Secure Hash Algorithm 1) SHA-2 hashing algorithms both are not time efficient but still not breakable and can be used by the developers. Regarding this, the authors in[7], have analyzed and juxtaposed the two most widely used algorithms which are Message Digest (MD5) and SHA and concluded that SHA hashing algorithms are easier to compute but are much harder to reverse and would take around millions of years to compute the authentic or veritable message content while MD5 is the message-digest algorithm that replaces its predecessor MD4.[8]

Secure Hashing Algorithm-256 is a cryptographic hash function that takes an input of the random size and produces an output of a fixed size. [9] SHA-256 was designed by the National Institute of Standards and Technology (NIST). Usually, hashing algorithms are used with other cryptographic algorithm or protocols to protect sensitive data. In our case, the developer has protected the public key using the AES algorithm. In addition, SHA-256 is given a fixed output value regardless of the input that is given in the first place. [3]

In 2012 the internet engineering task force organization has examined this algorithm to test the power behind it. In addition, the algorithm works base on key derivation which means it derives one or more secrete keys from a secret value such as passwords or a passphrase. Key deviation function proposed for low-memory setting.

AES is a symmetric key block cypher encryption algorithm and this algorithm was designed in 1998 by Vincent Rijmen and Joan Daemen and it is based on the Feistel network and supports 128-bit block size and key length 128, 192 and 256 bits. AES perform 10, 12 or 14 round and the number of rounds depends on the key. To illustrate, it performs 10 rounds for 128-bit key length and 12 rounds for 192-bit key length and lastly 14 rounds for 256-bit key length [10]. In advance encryption standard (AES) each round performs some steps. Key-expansion, initial rounds and final rounds. In the rounds step, Sub-byte generation, Shift-rows, Mix-columns and Addround_key are performed whereas, in the Final-rounds step, the same functions are performed except Mix-columns function.[3, 4]

DESIGN OF THE PROPOSED APPLICATION

The general architecture of the proposed solution along with its components is outlined in this section and depicted in

Figure 1. As observed in Figure 1, the user of the application will be able to perform various tasks once he/she runs the application. In addition, the system architecture shows the main three components of the system and each one of these components has a various mechanism work than others. These three main components are as follows:

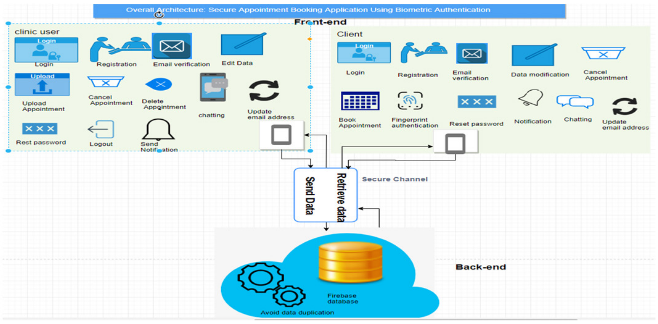


Figure 1: Overall architecture of the proposed application.

Front-end service

Front-end service is the user interface which will be displayed to the user whenever the user launches the application. Users will be able to interact with each other and forward a request to a remotely located back-end program on another device which in our case is the firebase database. The Figure 1 shows the proposed system front-end service separated down into two sections which are the customer and doctor interface. Each one of these front-end has many functions that user can interact with and perform the desired tasks efficiently.

Secure channel

The secure channel is the component that takes care of the data transformation which means the developer should protect the users' data and prevent information from leaking to third-party hand (Hacker). All data (Sensitive and non-Sensitive) will be passed through the secure channel. In addition, AES encryption and SHA-256 algorithms have been used for this purpose and implemented in the chatting function which will protect the user's messages and make end-to-end messages encryption. Furthermore, the CIA triad (Confidently, Integrity and Availability) including Authentication and authorization have been considered during app development and used wisely to protect the user data and safely keep their data. [5]

Back-end service

Back-end service is responsible for the business logic, performance and database interactions. In this case, the system data like the user's personal data, encrypted data and other data will be store in the database and then retrieve whenever the user interact and perform tasks with the application.

The proposed application functionalities will be listed and discussed in the following section:

A) Registration function

After downloading the application, the user (i.e. Doctor or Patient) will be allowed to sign up and create a new account. The users will have to fill in all the required fields such as username, email, password and phone number. By doing so, a new user will be created, and email verification will be sent to the registered email address. Aside from that, the doctor should upload the clinic license to confirm the registration process and consider his/her clinic as the authorized clinic.

B) Email verification function

The system will have an email verification function that allows newly registered users to verify their account through their signed-up email address. The main point of this function is to avoid anonymous users from accessing the system and only allow verified and authorized users to access and start performing different tasks.

C) Login and Logout function

The application will allow users to login into the system by using their previously registered credential such as email address and password. The application will check the validity of the users and only allows verified users to gain access to the system.[4,5]

D) Reset password function

In term of user accessibility, the reset password function is very important for users who forget their account password or getting into trouble during the login in process. The user will be able to send a request for a password reset by entering the registered email address, accordingly the system will respond with a reset password link sent to the registered email address.

E) Upload appointment function

The application will allow the user (doctor) to upload his/her available time slot to provide the patient with a choice to select the preferred available time slot and accordingly book the desired time slot easily and smoothly. [6,7]

F) List appointment function

This feature will allow the user (proprietor) to list all the uploaded appointments and accordingly check the booked and available appointments.

G) Delete, cancel and update appointment function

Through this feature, the user will be able to manage the appointments by deleting, cancelling or updating the booked appointments. There will be different buttons available for the user for each function i.e. deleting, updating and cancelling.[6]

H) Online live chat function with AES encryption

The proposed application supports a chatting channel that links between the different systems' users. This channel should be secure to keep user messages safely. The system will encrypt using Advanced Encryption Standard (AES) all the users' messages and save them in the database. Decryption will be done automatically upon users request for viewing the chat history.

I) Update user's email

Updating user's email is a feature that helps system's users to update their email address whenever they face trouble to reach their email. In addition, the application will allow only authenticated users to update their email address. This means users should authenticate with the system again and then only they will be allowed to update their email address.

J) Notification

The system will have a notification feature that notifies system users whenever an appointment gets booked or cancelled. Therefore, the system will have two types of notification which are onscreen notification and email-based notification.[7]

K) Book appointment with fingerprint authentication

This feature is considered the main function of the system. The mobile application will allow users (patient) to book any of the available appointments by placing their finger on the smartphone sensor to compare between the stored and the placed fingerprint pattern and assign the appointment as a booked appointment in case if the user fingerprint pattern matched, otherwise an error message will be displayed to the user, Figure 2.

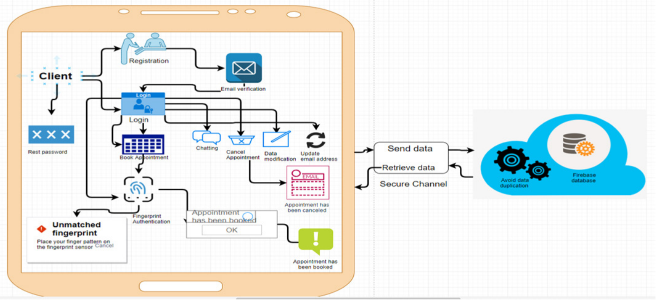


Figure 2: Operation architecture for the client user.

SYSTEM IMPLEMENTATION

The system implementation was done in two parts to properly manage and control the flow of information throughout the system and accordingly achieving both efficiency and security.[9] The first application which is called controller will manage doctor-side operations and will allow only registered doctors to open and manage their account in the system. In addition, the doctor should upload his/her medical license that proves the eligibility of working in the medical area. On the other hand, the second application which is the main appointment app, will be used by both users of the app i.e. the patient and the healthcare service provider for controlling and managing the appointments at both ends **(Figure 3,4)**.

The following section depicts some screenshots that were taken from the developed android application and displays some pages that users can navigate through when using the application. During the development process, screen resolution was also taken under consideration to make the system flexible and user friendly.[9,10]

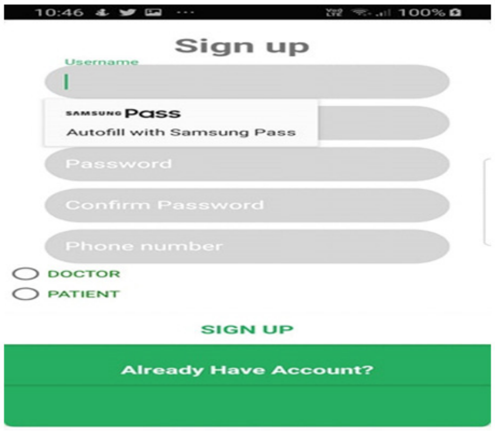


Figure 3: System sign up.

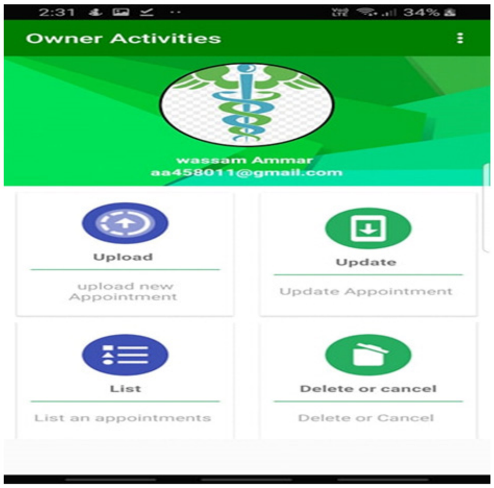
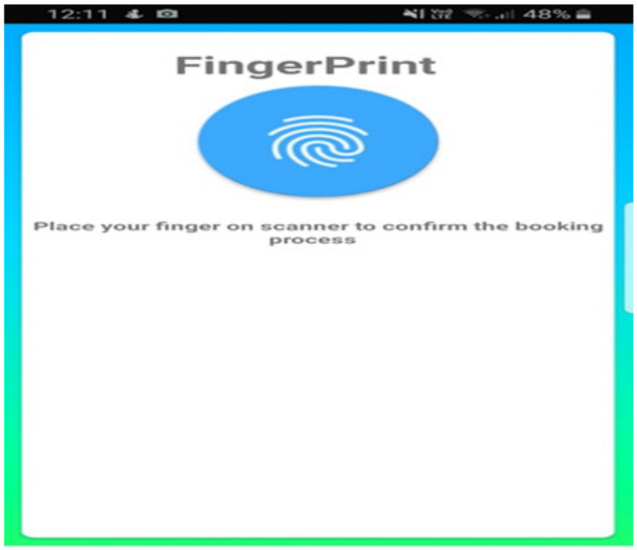


Figure 4: The controller App.

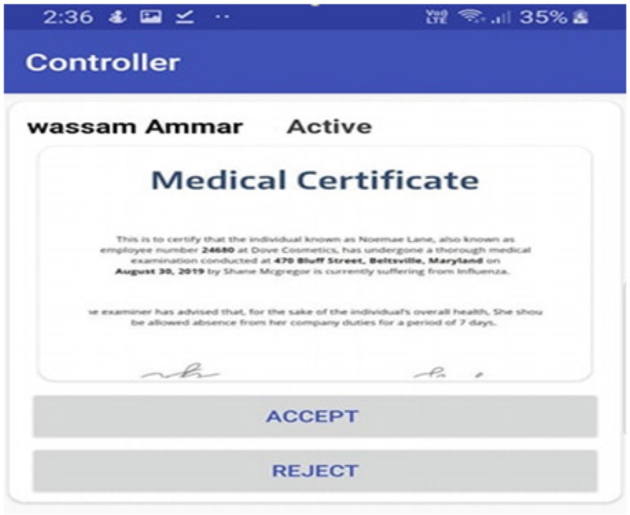
The controller application won't be published to the play store as it is used to activate or disable the account that is registered under the doctor's name or healthcare provider. In addition, the admin will have the ability to check the clinic medical certificate and take proper decisions based on the validity of the certificate (**Figure 5, 6**).[10]



FingerPrint

Place your finger on scanner to confirm the booking process

Figure 5: Fingerprint authentication.



wassam Ammar Active

Medical Certificate

This is to certify that the individual known as Noemae Lane, also known as employee number **24680** at Dove Cosmetics, has undergone a thorough medical examination conducted at **470 Bluff Street, Beltsville, Maryland** on **August 30, 2019** by Shane Mcgregor is currently suffering from Influenza.

ıe examiner has advised that, for the sake of the individual's overall health, She shou be allowed absence from her company duties for a period of 7 days.

Figure 6: Certificate of healthcare provider.

CONCLUSION

In conclusion, the main idea of the propped system is to automate the process of booking between the patients and doctors in an efficient and secure way. The solution also considered establishing a secure communication channel between the patient and the doctor. A comparison study between different encryption and hashing algorithms on mobile apps have been conducted to discover the weaknesses and strengths of each and then selecting the most suited encryption algorithm in terms of speed and security. The developed application used fingerprint authentication, AES encryption and SHA-256 hashing algorithm to achieve a high level of security with an efficient booking process. SCRYPT password algorithm has been adopted in the system to hash the user's password and save it safely and securely.

ACKNOWLEDGEMENT

The authors also wish to express gratitude to the management of Asia Pacific University of Technology & Innovation for their support.

Conflict of Interest

The authors involved in the current study does not declare any competing conflict of interest.

Funding and Sponsorship

No fund or sponsorship in any form was obtained from any organization for carrying out this research work

REFERENCES

1. Ravi S, Mankame DP. The multimodal biometric approach using fingerprint, face and enhanced iris features recognition. In2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT) 2013 Mar 20 (pp. 1143-1150). IEEE.
2. Misdan N, Ismail AF, Hilal N. Recent advances in the development of (bio) fouling resistant thin-film composite membranes for desalination. Desalination. 2016 Feb 15;380:105-11.
3. Kiah MM, Nabi MS, Zaidan BB, Zaidan AA. An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1. Journal of medical systems. 2013 Oct;37(5):1-8.
4. Jayabalan M, O'Daniel T. A Study on Authentication Factors in Electronic Health Records. Journal of Applied Technology and Innovation (e-ISSN: 2600-7304). 2019;3(1).
5. Hatzivasilis G, Papaefstathiou I, Manifavas C. Password Hashing Competition-Survey and Benchmark. IACR Cryptol. ePrint Arch.. 2015;2015:265.
6. Kumar EA, Blandi EN. A graphical password-based authentication based system for mobile devices. International Journal of Computer Science and Mobile Computing. 2014 Apr;3(4):744-54.
7. Aggarwal SR. What's fueling the biotech engine—2012 to 2013. Nature biotechnology. 2014 Jan;32(1):32-9.
8. Alanazi H, Zaidan BB, Zaidan AA, Jalab HA, Shabbir M, Al-Nabhani Y. New comparative study between DES, 3DES and AES within nine factors. arXiv preprint arXiv:1003.4085. 2010 Mar 22.
9. Zhang X, Hu H. Optimization of hash function implementation for bitcoin mining. In3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019) 2019 Apr (pp. 448-452). Atlantis Press.
10. Barfield C, Cornell J, Arbour J, inventors. Secure data storage system and method. United States patent US 8,201,261. 2012 Jun 12.