2019 FCI Final Year Project (Computer Science)

AUTOMATED AND PRIVACY PRESERVING E-ATTENDANCE SYSTEM BY USING BEACON FRAME ACTIVE SCANNING TECHNOLOGIES AND LIGHTWEIGHT DATA ENCRYPTION

UMS UNIVERSITI MALAYSIA SABAH

FACULTY OF COMPUTING & INFORMATICS
FAKULTI KOMPUTERAN DAN INFORMATIK

LEE YUNG SEN
BI17110176 | nelsonlee329@gmail. com

SV: DR TAN SOO FUN
soofun@ums.edu.my

ABSTRACTS

The regularity of student’s attendance is critical in the administration of higher Educational Institutions. Recently, the electronic attendance (e-attendance) system has been developed to assist in detecting of poor attendance. However, these E-Attendance systems are mainly constructed by using QR code technologies, i.e., Smart-Hadir e-attendance system in UMS. Several limitations were detected during the implementation of QR-based E-attendance system, includes (i) Fraudulence Scanning by the absent student; (ii) Camera condition and Lighting interference; (iii) inadequate to support active monitoring; (iv) Unauthorized access to redirected link; (iv) Lack of privacy protection for student data in E-Attendance system. To address this problem, this project aims to propose an Automated and Privacy Preserving E-Attendance System By using Beacon Frame Active Scanning Technologies and Lightweight Data Encryption. The use of beacon frame is its capability of advertising beacon signal by access point to search for nearby user devices before allowing them to join the network. This packet comprised of essential information of the device such as its MAC address, SSID etc. that can be utilized as unique fingerprint. To preserve data privacy, this project embeds the lightweight data encryption algorithm in securing low-end to high-end devices with almost negligible performance tradeoff when generating key to be exchanged with communicating entity (lecturer) as to ensure originality of the sent MAC address. The project will be utilizing an iterative method that consists of five phases such as requirement planning, analysis and design, development, testing and evaluation phase. The expected outcome of this project is delivering an automated and Privacy Preserving E-Attendance System, which can serve as an alternative solution to address the current limitation of the QR-based E-attendance system.

PROBLEM STATEMENTS

1. Student can impersonate other’s account and let them log in to the system
2. External light sources also degrade the dynamic range when zooming especially in bright condition.
3. Built-in QR camera library does now allow a simple pinch to zoom.
4. QR is not suitable for active monitoring purpose, the lecturer may need to reopen the QR code to authenticate against the presence of student.
5. Unprotected communication over the intermediary device could lead to potential privacy breach due to spoofing attack.

OBJECTIVES

1. To investigate a Lightweight Data Encryption Algorithm and Beacon Frame Wireless LAN technologies for developing an automated and privacy preserving E-attendance system
2. To investigate a Lightweight Data Encryption Algorithm and Beacon Frame Wireless LAN technologies for developing an automated and privacy preserving E-attendance system.
3. To test and evaluate the proposed automated and Privacy Preserving E-Attendance system by using the simulation case study approach.

DESIGN & IMPLEMENTATION

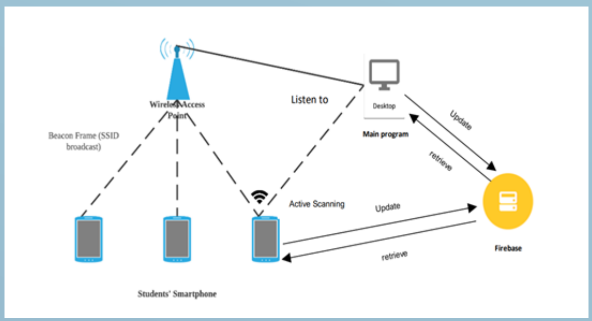


Figure 2 – Testbed Overview

The overview topology of system shown in Figure 2. it will be implemented using available wireless access point and a laptop or desktop in the lab. A main program will be installed into the computer, set up the database and kismet. Student will bring their smartphone to the class.

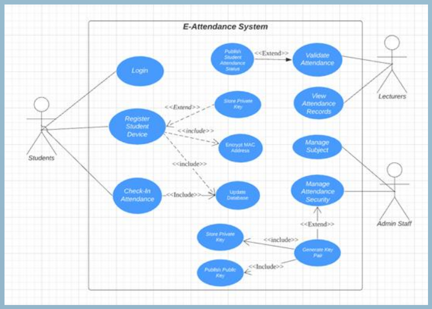


Figure 3 – Use Case Diagram

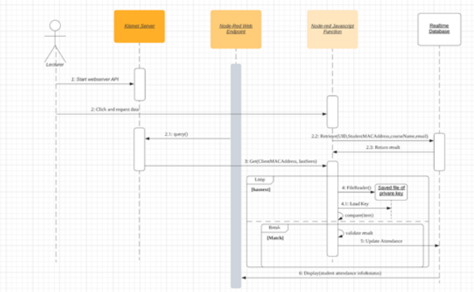


Figure 4 – Sequence Diagram for attendance validation

METHODOLOGY

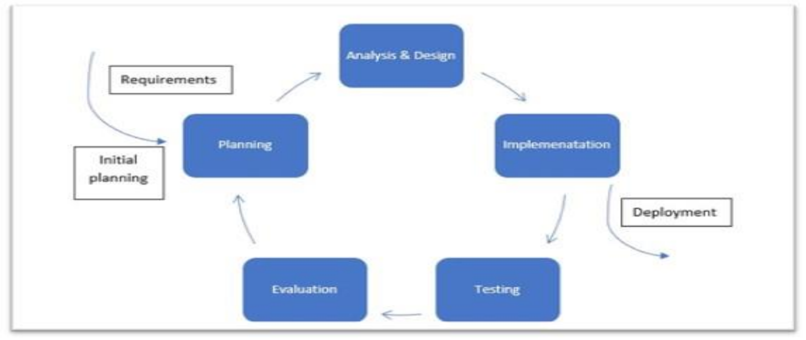


Figure 1- Iterative development

The reason to choose this methodology that focuses in exploring the potential for the existing technology need to be learnt by the author while working on the project.

Process of Iterative Model comprised of 5 phases unlike to the most popular model such as waterfall, the difference is in which steps are repeated or cyclic and each completion of each cycle incrementally as shown in Figure 1.

RESULT

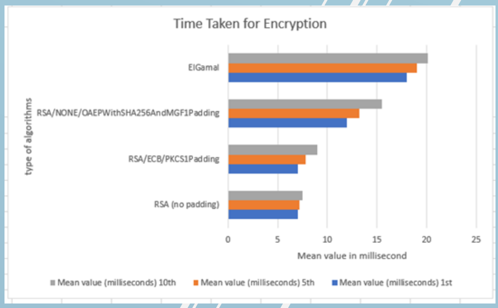
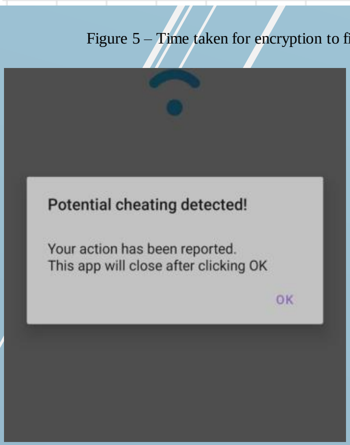


Figure 5 – Time taken for encryption to finish

Figure 5 shows The graph shows the number of trials and the average time taken in millisecond for each algorithm padding excluding ElGamal. As shown in the graph, the longest time taken was ElGamal recorded at 20.1 milliseconds and as well for the third round of each padding types.



Potential cheating detected!

Your action has been reported.
This app will close after clicking OK

Figure 6 – Fraudulent Scanning Detection

Figure 6 shows student made changes to the MAC address with someone else account, the application is integrated with fraudulent checker and it is limited to individual who owns the phone. Afterwards, application downloads a snapshot of user data that contains previously registered MAC address, which then a comparison is made, the result is not equal leading to a warning message comes out stating that potential cheating detect and subsequently, violation of attendance rule is expected.

CONCLUSION

The final deliverable project is an automated and privacy preserving e-attendance system by using beacon frame active scanning technologies and lightweight data encryption. The term for automated means involvement of human efforts is minimal and the whole process is handled by the system with only short amount of time to take attendance. This implementation emphasizes on fraudulent attendance system in order to maintain a valid record of attendance effectively. With the help of encryption, MAC address of the device is concealed when transmitted over the open channel, and only the right people have the knowledge of it.