Four-Factors Authentication Algorithm For Preventing Fake Attendance

Asim Balarabe Yazid
Computer Science Department
Nile University of Nigeria
asimbyazid@nileuniversity.edu.ng

Moussa Mahamat Boukar, PhD
Computer Science Department
Nile University of Nigeria
musa.muhammed@nileuniversity.edu.ng

Salisu Yusuf Ibrahim
Computer Science Department
Nile University of Nigeria
salisu.yusuf@nileuniversity.edu.ng

Isa Muslu, PhD
Computer Science Department
International Alatoo University
imuslu2001@gmail.com

***Abstract*— Taking attendance is a day-to-day chore for every organization, human resources, and class teachers, traditionally people take attendance manually either by calling out names or allowing the user to sign the attendance sheets or clock in and out. The problem, however, people most likely sign the attendance on behalf of their colleagues that are absent. This makes the traditional method very vulnerable and may affect the integrity of the system. Researchers come up with different ideas and methods of minimizing fake attendance to improve efficiency in terms of integrity, time and cost. After reviewing the existing system's strength and vulnerabilities, we are proposing a multi-factor authentication algorithm which makes use of QR code, GPS, and Facial recognition. The user will make use of their personal mobile phone. The research of this proposed is still ongoing, we are hoping the proposed technique can be applied to various attendance systems such as schools, universities, and organizations.**

Keywords— Attendance, QR code, GPS, Face Recognition, Timestamp, authentication

I. INTRODUCTION

There are different ways of authentication deployed by many researchers which are categorized into three (Asim, Moussa and Salisu 2018). The identity based authentication; This authentication identify the object based on who that person is by using biometrics such as finger print, facial recognition and retina scan. Identity based authentication is very difficult to compromise. The knowledge based authentication relies on memory, such as alphanumeric password, such that the system can be able to remember the person. This means the user can authenticate anyone with the password. Lastly Ownership authentication is based on what you have, such as ATM card or RFID. All the authentication mentioned above have their pros and cons but mostly depends on what will solve your problem (Asim, Moussa and Salisu 2018).

II. LITERATURE REVIEW

Android mobile phone application was used to simulate the proposed system by(Sunil, et al. 2018).

The system uses QR code which sends the data to the teacher's online page where all attendance are being recorded.

The proposed system in (Miran 2014) was aimed at improving student's regular attendance such that student can be able to monitor their own attendance in order to avoid penalties. The teacher will mark the absentees of the class manually on a paper, then pass the record to system manager, then performs manual calculation and post a list in which a student can be able to retrieve his attendance information through QR code. The entire system is slow because it is not fully automated, a lot of paper work, requires data entry personnel, records may have lost and many more.

This proposed system uses face detection, machine learning and GPS in order to mark the presence of a student. The GPS technology was used to avoid veracious attendance; student needs to be within the radius of the class before he/she can be able to authenticate. At some point, student may have a genuine excuse of not attending the class, so at this point the student will have to prove his/her presence by using the same GPS technology. Integrity of system is difficult to compromise (Nabil , Bhawna and Sadia 2014).

Student will make use of mobile device scanning through a QR code on a computer screen, the system will record the attendance and the teacher can be able to generate and print attendance report. No effort of preventing veracious or fake attendance (Md Rizal, Mohd and Afzaal 2017).

Their system identifies the common vulnerabilities of existing proposed systems; the technique was aim to avoid users who will try to compromise through fake attendance. That is actually a serious problem when it comes to the integrity of the system. IMEI was used as means of identification, QR code as token, timestamp and lastly GPS to identify student location. The system is very efficient in terms of usage and cost. The limitations include student at the corner side of the class finds it difficult to authenticate when QR code is displayed on a projector. The system integrity of the system relied on the location of the student's mobile phone not to the

978-1-7281-5160-1/19/$31.00 ©2019 IEEE

student himself, which makes the system vulnerable (Yew , Khairul and Serdarmammet 2018).
The authors proposed QR code attendance system using mobile application in order to solve the problem of cost efficiency or as an alternative to other proposed systems such as RFID. The authors make use of OTIP and QR code. They claimed their system is able reduce dishonest attendance (Cho and Mi-Young 2014).
The authors proposed a multi-factor attendance system which efficiently record the attendance of the users, by using GPS to know the location of the student and student will need to make a facial capture using the phone app camera before using the QR code. So that the teacher can be able to compare or match the student with the record stored on the server. The limitation of the system has to do with the teacher manually matching the faces of the student after class hours. Which makes the proposed system less time effective (Fadi and Nael 2014).
QR code technology was used as a token, GPS and timestamp was used to make sure the student is within the premises and presence during the class period. The system has an excellent evaluation score during user test. The system vulnerability happens when a student can mark his fellow student presence as long as the student is in possession of the fellow student's mobile phone (Zakiah, et al. 2018).
The proposed system by (Rishab, et al. 2018) sends parent notification after the student sign in to the class. The teacher has to scan the QR code before student attendance will be confirmed. The system eliminates false registration by users.

III. METHODOLOGY

User Authentication
Preventing user from taking fake attendance or signing attendance on behalf of their fellow colleagues is very difficult, most especially when the population of the people in the class or organization is very high.
In order to prevent fake attendance, certain thing has to be in place.

1. The user must be sign the attendance during the class hours
2. The user must be present in the class or within the school premises.
3. The user must take the attendance.
4. The user must only sign one attendance at a time.

In this paper we combine and optimize four authentication factors to achieve this result.
The system will make sure the student is in class my getting the student's geographical location using GPS and comparing it with that of the classroom. If the user is not within the premises, the system will not proceed to the next phase. When the system confirms his presence then the mobile application will proceed to the second phase by scanning the user's face. This authentication will allow us to confirm the identity of the student. Lastly the user will use the primary camera of his/her mobile application to scan the QR code projected by the lecturer which serves as a token and signature. Once the the student sign the information will be stored online with a timestamp of the time the student takes the attendance.

System Design
The figure 1 describes the activity flow of the proposed system.

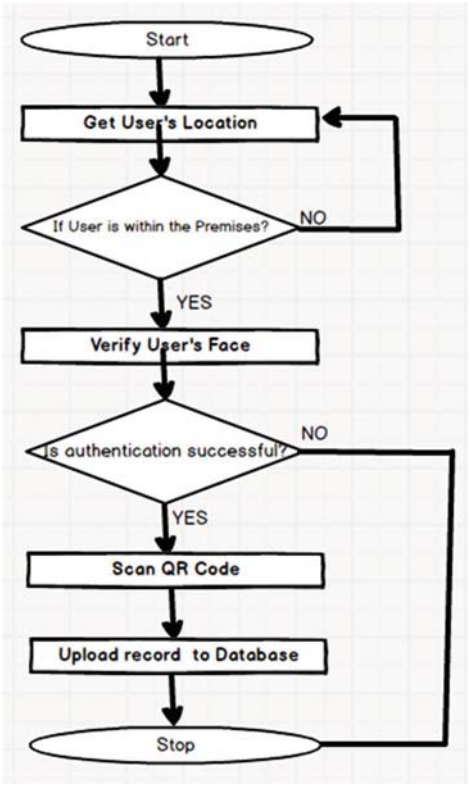

Fig .1 Activity Diagram

IV. CONCLUSION

The system was aimed at optimizing the existing system, and improve the integrity of the information by preventing fake attendance. Some existing work focused more on the detection of fake attendance, but in this research we prove that preventing is more important than detection. This algorithm does not require any extra software or hardware tool. The simulation and the test proves that the algorithm can be applied in different areas.

V. REFERENCES

Asim, Balarabe Yazid, Mahamat Boukar Moussa, and Ibrahim Yusuf Salisu. "PandaLock: Variable-Pointer Rotary-password authentication Technique." *14th Interntational Conference on Electronics Computer & Computation ICECCO 2018.* 2018.
Cho, Dae-Jea, and Bae Mi-Young. "International Journal of Multimedia and Ubiquitous Engineering." *A study on Development of OTIP system using QR code based on Smartphone.* 2014.
Fadi, Masalha, and Hirzallah Nael. "A Students Attendance System Using QR Code." *International Journal of Advanced Computer Science and Applications,.* 2014. 75-79.
Md Rizal, Md Hendry, Noah A Mohd, and H. Seyal Afzaal. "Smart Attendance System Applying QR Code." *12th International Conference on Latest Trends in Engineering and Technology (ICLTET'2017).* Kuala Lumpur (Malaysia), 2017.
Miran, Hikmat Baban. "Attendance Checking System Using Quick Response Code For Students At The University Of

Sulaimaniyah." *Journal of mathematics and computer science.* KRG-Iraq, 2014. 189-198.
Nabil , Litayem, Dhupia Bhawna , and Rubab Sadia. "Automatic Attendance and Mobile Learning System in Sensor Enabled Heterogeneous and Dynamic University Environment." 2014.
Rishab, Agrawal, Patil Megha, Ingle Snehal, and Shete S. A. "QR Code Attendance using Web Browser." *International Journal for Scientific Research & Development.* Pune-India, 2018. 712-714.
Sunil, Jadhav, Gagare Akash, Gunjal Pooja, and JagTap Vidya. "Android Based Smart Attendance System using QR Code." *International Journal of Innovative Research in Computer and Communication Engineering.* Ahmednagar: IJIRCCE, 2018.
Yew , Kwang Hooi, Shafee Khalid Khairul , and Tachmammedov Serdarmammet. "Multi-Factor Attendance Authentication System." *International Journal of Software Engineering and Computer Systems (IJSECS).* Malaysia Pahang, 2018. 62-79.
Zakiah, Ayop, Lin Chan Yee, Anawar Syaulnaziah, Hamid Erman, and Syahrul Muhammad. "Location-aware Event Attendance System using QR Code and GPS Technology." 2018. 466-473.

978-1-7281-5160-1/19/$31.00 ©2019 IEEE

978-1-7281-5160-1/19/$31.00 ©2019 IEEE