Randomized QR-code scanning for a low-cost secured attendance system

Muhammad Imanullah, Yuza Reswan
Department of Engineering, Universitas Muhammadiyah Bengkulu, Bengkulu, Indonesia

Article Info	ABSTRACT
	Human resource management requires good documentation and good data processing. In workspaces such as offices and factories, employee salaries are determined by calculating attendance at each hour of work. Tracking and collecting attendance data for a large number of employees is a difficult thing to do. We need a secure system to facilitate the process of collecting and tracking presence data. We propose an attendance system that uses random quick response code (QR-codes) as one time password (OTP) to improve security. Employees are required to scan the QR-code within ten seconds before it is changed and randomized each time. The proposed attendance system facilitates data collection using employees' smartphones and Mac-Address as unique identification numbers. The system is able to track employees' arrival and departure times. We have implemented the system at the local university to collect lecturer attendance data then analyze its security and statistic in all scanning activities. The average time needed by a user to authenticate their presence in the system is 25.8877 seconds. The steps needed to sign in and out from the system are fewer than other previous researches. Those findings tell us that the approach is straightforward and more uncomplicated than other proposed methods. We conclude that randomized QR-code scanning is a relevant scheme to be applied in a secure attendance system.

Corresponding Author:

Muhammad Imanullah
Department Engineering, Universitas Muhammadiyah Bengkulu
Bali street, Postal Code 38119, Bengkulu, Indonesia
Email: muhammad.iman@umb.ac.id

1. INTRODUCTION

Attendance is one of many important aspects that concern many leaders in the work community towards the workers they lead. Many organizations determine the employee's honor by their attendance on each business day. According to statistical findings in [1], an increase in salaries is significantly related to labor supply with about -0.04 of elasticity. That finding shows that higher salaries will not always be linearly connected to the increase in worker attendance. They have valid reasons for wanting the improvement in quality of working life through attendance and reducing the absenteeism using some strategies as stated in [2]. With the workers' attendance data, the organization will be able to cut unnecessary expenses and determine different honors for each worker. Like in [3], attendance data is obtained using the attendance/absenteeism sheet to determine the number of allowable non-productive hours (vacation, holidays, and sick leaves) to finally result in replicating the monthly salary budgets for nursing personnel. Hence, a system that is able to collect attendance data quickly and precisely is needed.

There have been lots of efforts done by researchers in building attendance systems. The effort of building an attendance system can be started with many approaches (a wide variety of methods, tools, and

subjects). Those approaches vary in the security aspect, accuracy aspect, and actualization of data. Like in [4]–[9], radio-frequency identification (RFID) is used to provide a robust, scalable, secure, and automatic attendance system. Those RFID approaches are requiring workers to bring the ID device to work so the attendance system can identify them and automatically fill the attendance data. To tackle the need of bringing ID devices to work every time, other approaches that make use of the biometric ID are proposed by researchers. With biometrics, the interaction between workers and the attendance system becomes more effective and efficient. Biometrics that uses body measurements and calculations is intended to explain the characteristics of the human body in a formal mathematical way. Some attendance systems use biometric to identify their users. Those biometric attendance systems using fingerprint [10], iris [11], face [12], or voice [13]. A biometric based attendance system is a very promising method to adopt for future needs but it still has some security issues as people can alter the image taken by biometric sensors. An altered image taken by a biometric attendance system can make the computer misidentify a person, and that leads to a chance of cheating among the workers. To minimize the chance of cheating and to have a reasonably secure system, quick response code (QR-code) scanning is proposed. Some researchers like [14]–[16], using QR-code to identify a person or encapsulate some messages to achieve some goals. With QR-code scanning as an identification statement, we can reach a secure and robust attendance system where users are not required to bring any identification device other than their own smartphone. Workers nowadays are attached to their smartphones, so they will always need and want to bring them anywhere, and not feel obligated to do it. That is the main reason for us to use QR-code scanning as an identification method. What differentiates our QR-code based attendance system from others is the straightforwardness and fewer usability steps.

As stated in [17], we can divide authentication into three methodologies: something you have (RFID device), something you know (personal information number (PIN), and password), and something you are (biometrics). Though the combination of those three authentication methodologies will serve us the highest security, we can actually use only one that meets our environmental needs. This research focuses on utilizing the use of QR-code to find a better method in securing the attendance data. QR-code scanning is still a relevant way of identifying users securely as it can be found in the popular system like Facebook, Telegram, and WhatsApp. Our system is able to acquire attendance data using the same principle found in the WhatsApp web application.

2. RESEARCH METHOD

We require a secure and controllable transfer data mechanism to build our attendance system. We propose a method called randomized QR-code scanning to achieve it. With the combination of QR-code and network configuration, we try to increase the system security. Figure 1 shows our attendance system scheme running on a local network where the user can directly communicate with the server. The first step for the user to use the attendance system is being connected to a local network. Once user is connected, they are required to open the android application to scan the randomized QR-code provided by the server app. The android application has a simple look and has only two main buttons to sign in and out. When the scanning process is done, a packet containing identifier data is sent from the user's smartphone to the server app. The server app will receive and process the packet sent by the user through the local network. At last, users are succeeded to sign their attendance while the server always randomizes the QR-code every 10 seconds for security manner. The system is evaluated through 100 test scenarios where users are required to authenticate their presence by connecting to the local network, running the android application, and signing in. The questionnaire form is also used as an evaluation tool to obtain feedback from participants about the system. The test results are shown as statistical graphics in the result and discussion section along with some discussion materials obtained from participants' feedback.

2.1. Network

We set up our attendance system in a local network as a requirement for users to be present in a specific location (workplace) and specific time (work-hours). This requirement will prevent users to cheat, like signing in from outside of the workplace. The communication between users and the server is done through transmission control protocol (TCP). According to [18], TCP has less packet delay and less packet loss over user datagram protocol (UDP), hence we use it as our main data transfer protocol. The server will have a static IP address so users can communicate with it easier without having to change the destination IP address every time they connected to the network.

2.2. Unique identification

Many systems that involve users and sensitive data require unique and secured identification. Like a proposed system in [19], the fingerprint is used as an identification key while QR-code is used as a mark to verify the user's attendance in a physical train seat. Another system in [20], introduced a secure course

attendance system using the face as an identification key and QR-code to encapsulate some courses detail information. What differentiates our proposed system from earlier researches is the combination of media access control (MAC) address as a unique identification key and QR-code as a security key to authenticate user's attendance. We use MAC address since it is word-wide unique [21]. Which means that each smartphone user in the world will have a different 12-digit hexadecimal number (6-Byte binary number), represented in colon-hexadecimal notation, hyphen-hexadecimal notation, or period-separated hexadecimal notation. Using MAC addresses as unique identification to differentiate one user from another has been our best choice. Within our research processes, many participants showed the dissent to give their international mobile equipment identity (IMEI) or phone number as an identification number. MAC address is not too sensitive compared to IMEI and phone number, so we can use it on a public occasion.
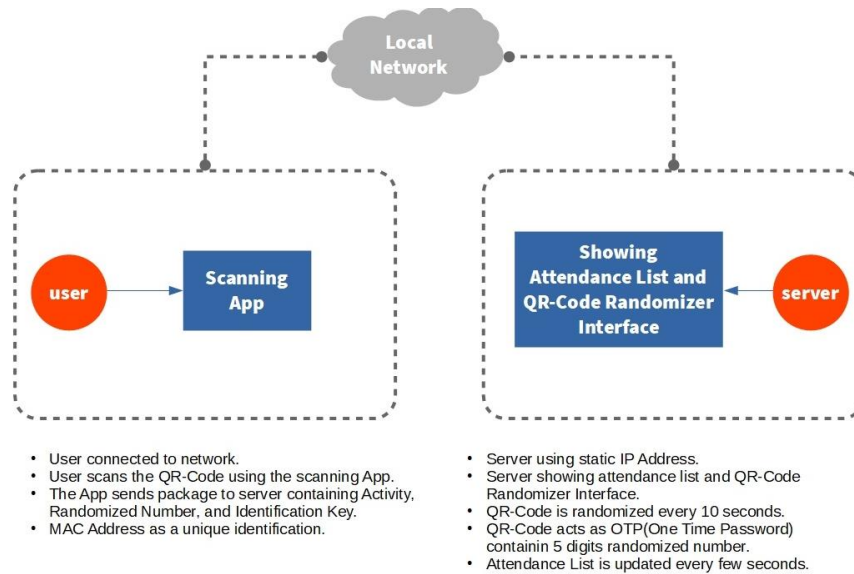

Figure 1. Attendance system scheme

2.3. QR-code Scanning

Our proposed method is centered on the activity of QR-code scanning and the exchange of encapsulated security key and attendance data between user and server. The server will generate QR-code containing a five digits randomized numbers as shown in Figure 2. This randomized number is acting as one time password (OTP) which appears to be a robust and secure solution in many sensitive data transactions such as electronic payments [22], online transactions [23], secured data accessing systems [24], and corporate information systems [25]. Each digit is filled with a random number from zero to nine. The QR-code containing five digits randomized number are generated every ten seconds to prevent alteration from the cheating user. QR-code scanning is a quick method for entering the OTP since users are not required to type the number each time.
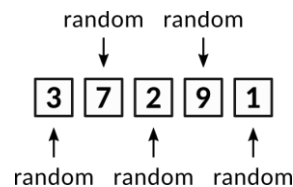

Figure 2. Randomized number as OTP

A user who scans QR-code will send a packet of the message containing the randomized number along with other information as shown in Figure 3. Delimiters are used to ease the data parsing. The packet is sent to the server using TCP over a local network. The server will identify users by their MAC address and

check the randomized number whether it is matched or not. If the randomized number sent by the user is not similar to what the server has, then the user is failed to authenticate their attendance.
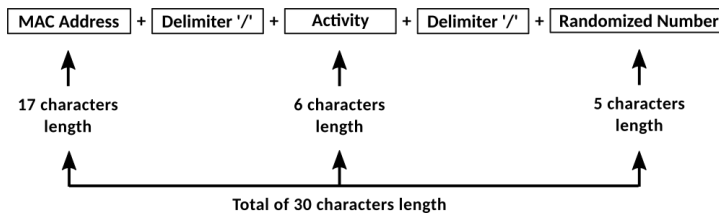

Figure 3. Information packet send through TCP

3. RESULTS AND DISCUSSION

Our proposed scheme is inspired by real office life needs. The scheme is made to enhance an attendance system's security. We implemented it in a university attendance system containing real lecturers data. In some universities, lecturer presence is needed in determining basic teaching honor. Attendance system collecting data of presence time, departure time, and teaching info. Those data can be analyzed to statistically tell us about the lecturer's discipline.

One of many things to do firstly in building an attendance system is designing a database. Figure 4 shows our database design which contains only 4 tables. The database is designed in a simple form to make it straightforward and easy to use. Pre-collected data are lecturer info, teaching schedule, and college room info. For daily use, lecturer presences are stored in a daily presences table.
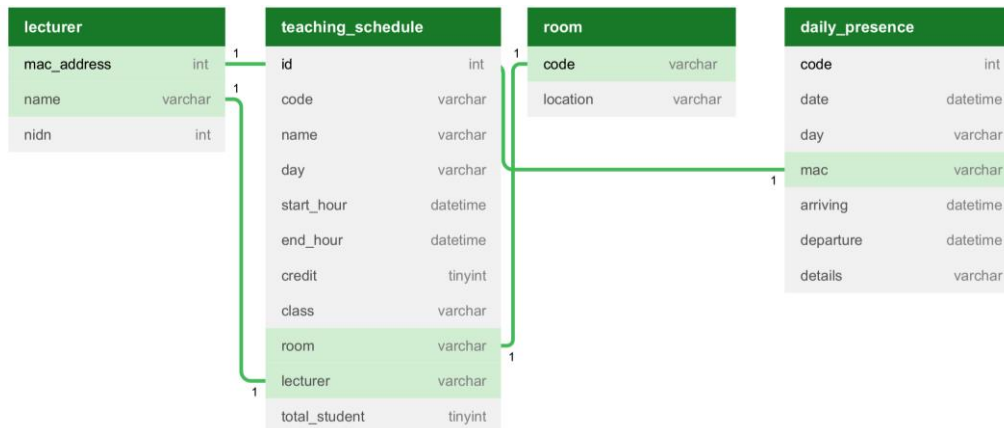

Figure 4. Database design

As an information serving and presence recording system, our attendance system is designed with a simple interface. The Server App system is released as Desktop App as shown in Figure 5(a) which is able to present main information in the common monitor, big screen, or projector. Figure 5(b) shows the user interface layout. The header contains the university logo, date, and time information. The main body contains the teaching schedule and lecturer presence. The footer contains the current process status, and the sidebar contains randomized QR-code and announcements.

The android application which acts as mobile scanning app also has a simple layout. Released in android, this scanning app only has two buttons as shown in Figure 6(a). Users are expected to quickly understand the workflow and scanning activity. Figure 6(b) shows the QR-code scanning interface while Figure 6(c) shows the scanning activity. Users are required to register their MAC address into attendance system before being able to use it. Once users are registered, they can authenticate their presence by connecting to the workplace network and scanning the QR-code using a mobile scanning app. Their presence in the workplace network becomes one of many security efforts to prevent a user from cheating. QR-code acts as an OTP, and it will be randomized every 10 seconds to prevent a user from sending an unauthorized packet of data to the system.
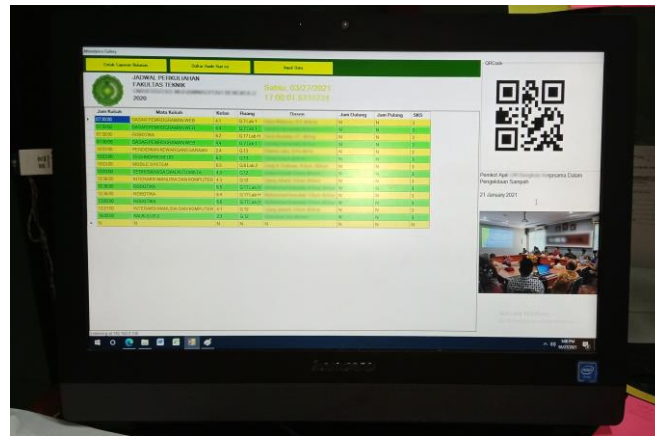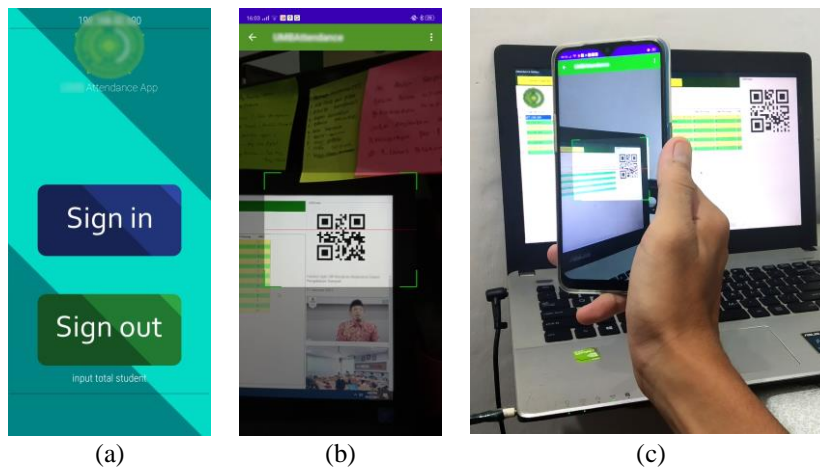
(a)
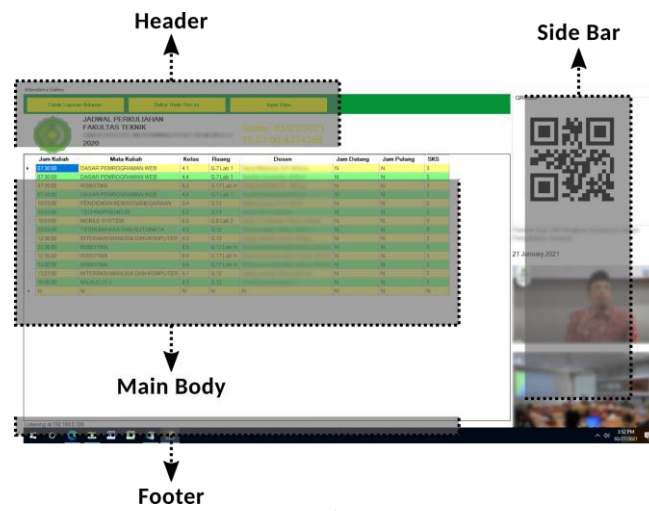
(b)

Figure 5. Desktop app interface (a) installed in all in one PC and (b) app layout

(a)　　　　　(b)　　　　　(c)

Figure 6. Android app interface: (a) app layout, (b) scanning interface, and (c) scanning QR-code activity

The steps required by users to authenticate their presence and departure are shown in Figure 7. The steps are fewer than other previous researches. Like in [26], users are required to log into the app using a username and password before being able to scan the QR-code and record their attendance. And also in [27],

users are required to scan QR-code printed on their ID card followed by extra authentication using their fingerprint or voice before being able to record their attendance. With fewer steps, we try to present a simpler and straightforward attendance system. For further development of a secured attendance system, we actually believe that extra authentication using biometric is necessary and needed.

We have run 100 test scenarios to measure how much time is needed by users to authenticate their presence (in seconds) from connected to the local network, running the app, and signing in. Figure 8(a) shows the test value for each user while Figure 8(b) shows the sorted statistic version with a blue line as an average value. From all measurements with a minimum value of 13.64 seconds and a maximum value of 43.03 seconds, we got an average time of 25.8877 seconds. Some attempts that require maximum time are mostly caused by technical errors due to package loss over TCP communication. The average time of 25.8877 seconds is reasonable for a secured system where every required to be present in the local workplace network while using their own smartphone. It also validates our claim on the straightforwardness of the system. Besides some positive feedback about the simplicity and straightforwardness of the system, some critical feedback was also obtained using questionnaire forms filled by participants. That feedback is mostly targeted around the use of MAC address as an authentication method which is vulnerable. Participants are concerned, knowing that people can easily get the fake MAC address using some apps to cheat the system. Some other feedback also suggested us to change the communication scheme into a global network as it will give the system more accessible to wider usage.

Figure 7. Presence authentication steps
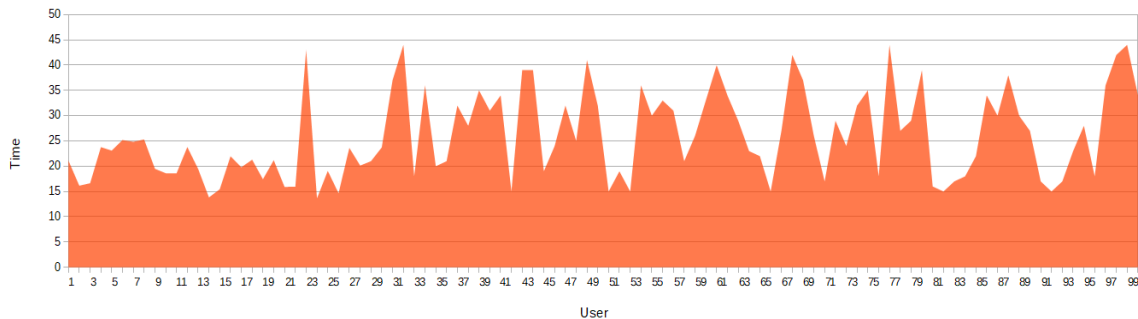
(a)
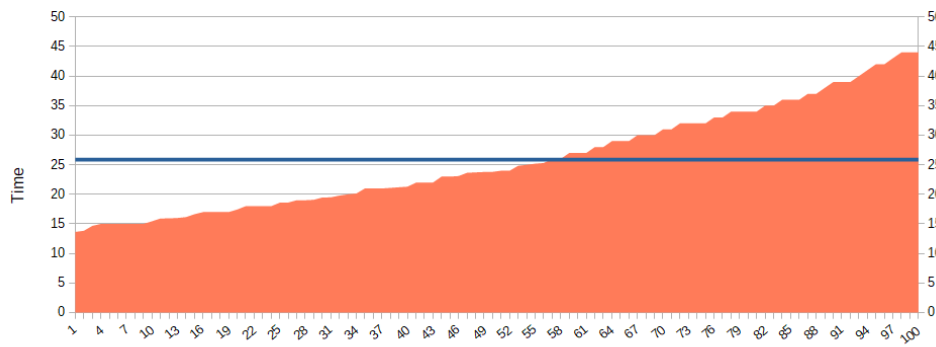
(b)

Figure 8. Test data statistics: (a) time needed by 100 users to authenticate their presence (in seconds) and (b) sorted version of all test data

4. CONCLUSION

Test scenario shows that the proposed scheme utilizing QR-code as an OTP to improve security in an attendance system, works very well. Users are required to be present in the workplace area and scan the QR-code within 10 seconds, so it eliminates the chance of cheating. The average time needed by a user to authenticate their presence in the system is 25.8877 seconds. The steps needed to sign in and out from the system is fewer than other previous researches. QR-code scanning is a quick method for entering the OTP since users are not required to type the number each time. Those findings tell us that the system is straightforward and simpler than other proposed methods. We conclude that randomized QR-code scanning is a relevant scheme to be applied in a secure attendance system. Other than that, it also has big potential to improve many information systems on many occasions. MAC address is used within our system to facilitate easy and unique identification info but turns out it does not give us a reliable solution since it can be hacked in some ways (fake MAC address). For future development, we consider enhancing the security by using other authentication factors like biometric.

REFERENCES

[1] N. Mocan and D. T. Altindag, "Salaries and work effort: an analysis of the European Union Parliamentarians," *The Economic Journal*, vol. 123, no. 573, pp. 1130–1167, Dec. 2013, doi: 10.1111/ecoj.12056.

[2] R. Thérault, P. B. Lesage, and M. Boisvert, "Absenteeism: importance, nature and remedies," (in French), *Relations industrielles*, vol. 36, no. 4, pp. 775–802, Apr. 2005, doi: 10.7202/029204ar.

[3] N. Gheith, A. M. Zakaria, and S. H. El-Sayed, "Cost of nursing care for endoscopy patients in endoscopy unit at specialized Medical Hospital-Mansoura University," *Australian Journal of Basic and Applied Sciences*, vol. 3, no. 3, pp. 2038–2047, 2009.

[4] A. G. Putrada and M. Abdurohman, "Increasing the security of RFID-based classroom attendance system with shamir secret Share," *International Journal on Information and Communication Technology (IJoICT)*, vol. 6, no. 1, Jun. 2020, doi: 10.21108/IJOICT.2020.61.480.

[5] Q. Miao, F. Xiao, H. Huang, L. Sun, and R. Wang, "Smart attendance system based on frequency distribution algorithm with passive RFID tags," *Tsinghua Science and Technology*, vol. 25, no. 2, pp. 217–226, Apr. 2020, doi: 10.26599/TST.2018.9010141.

[6] G. D. P. Maramis and P. T. D. Rompas, "Radio frequency identification (RFID) based employee attendance management system," *IOP Conference Series: Materials Science and Engineering*, vol. 306, no. 1, Feb. 2018, doi: 10.1088/1757-899X/306/1/012045.

[7] H. D. Rjeib, N. S. Ali, A. Al Farawn, B. Al-Sadawi, and H. Alsharqi, "Attendance and information system using RFID and web-based application for academic sector," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, 2018, doi: 10.14569/IJACSA.2018.090137.

[8] H. El Mrabet and A. Ait Moussa, "IoT-school attendance system using RFID technology," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, no. 14, Aug. 2020, doi: 10.3991/ijim.v14i14.14625.

[9] M. I. Younis, Z. F. A. Al-Tameemi, W. Ismail, and K. Z. Zamli, "Design and implementation of a scalable RFID-based attendance system with an intelligent scheduling technique," *Wireless Personal Communications*, vol. 71, no. 3, pp. 2161–2179, Aug. 2013, doi: 10.1007/s11277-012-0929-3.

[10] Akinduyite C.O, Adetunmbi A.O, Olabode O.O, and Ibidunmoye E.O, "Fingerprint-based attendance management system," *Journal of Computer Sciences and Applications*, vol. 1, no. 5, pp. 100–105, Nov. 2013, doi: 10.12691/jcsa-1-5-4.

[11] S. Kadry and M. Smaili, "Wireless attendance management system based on iris recognition," *Scientific Research and Essays*, vol. 5, no. 12, pp. 1428–1435, 2010.

[12] A. S. Alon, "A YOLOv3 inference approach for student attendance face recognition system," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 2, pp. 384–390, Feb. 2020, doi: 10.30534/ijeter/2020/24822020.

[13] S. Nidhyananthan, R. S. S. Kumari, and S. Selvi, "Text-independent voice based attendance system under multi-speaker and noisy environments," *Australian Journal of Basic and Applied Sciences*, vol. 8, no. 13, pp. 121–131, 2014.

[14] D. S. Zingade, V. Jangade, A. Varade, M. Sable, and S. Shirsat, "The automated system for general administration using QR code," *International Journal of Advance Engineering and Research Development*, vol. 3, no. 2, pp. 23–26, May 2018, doi: 10.21090/IJAERD.RTDE28.

[15] A. A. Emmanuel, A. E. Adedoyin, O. Mukaila, and O. O. Roseline, "Application of smartphone QRcode scanner as a means of authenticating student identity card," *International Journal of Engineering Research and Technology*, vol. 13, no. 1, Jan. 2020, doi: 10.37624/IJERT/13.1.2020.48-53.

[16] C. Maciel, V. Carvalho Pereira, C. Leitão, R. Pereira, and J. Viterbo, "Interacting with digital memorials in a cemetery: insights from an immersive practice," Oct. 2018, doi: 10.5753/ihc.2018.4229.

[17] M. Galterio, S. Shavit, and T. Hayajneh, "A review of facial biometrics security for smart devices," *Computers*, vol. 7, no. 3, Jun. 2018, doi: 10.3390/computers7030037.

[18] Y.-C. Lai, A. Ali, M. S. Hossain, and Y.-D. Lin, "Performance modeling and analysis of TCP and UDP flows over software defined networks," *Journal of Network and Computer Applications*, vol. 130, pp. 76–88, Mar. 2019, doi: 10.1016/j.jnca.2019.01.010.

[19] B. Muthukumar, J. Albert Mayan, G. Nambiar, and D. Nair, "QR code and biometric based authentication system for trains," *IOP Conference Series: Materials Science and Engineering*, vol. 590, Oct. 2019, doi: 10.1088/1757-899X/590/1/012010.

[20] D. Sunaryono, J. Siswantoro, and R. Anggoro, "An android based course attendance system using face recognition," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 3, pp. 304–312, Mar. 2021, doi: 10.1016/j.jksuci.2019.01.006.

[21] GeeksforGeeks, "Introduction of MAC address in computer network," geeksforgeeks.org. 2020. https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/ (accessed Mar. 06, 2021).

[22] M. A. Hassan, Z. Shukur, and M. Kamrul, "An improved time-based one time password authentication framework for electronic payments," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020, doi: 10.14569/IJACSA.2020.0111146.

[23] S. S. Reddy, "OTP on GPS: an enhancement to OTP security model for securing On-Line transactions," *International Journal for*

Research in Applied Science and Engineering Technology, vol. 6, no. 7, pp. 767–770, Jul. 2018, doi: 10.22214/ijraset.2018.7129.

[24] F. Noorbasha, C. R. Krishna, and S. HafijullaIrshad, "FPGA based OTP generation system for data security," *International Journal of Recent Technology and Engineering*, vol. 8, no. 5, pp. 1836–1839, Jan. 2020, doi: 10.35940/ijrte.E4879.018520.

[25] V. Landyshev, T. Blinovskaya, and D. Krakhmalev, "The practice of using one-time passwords in modern corporate information systems," *E3S Web of Conferences*, vol. 224, Dec. 2020, doi: 10.1051/e3sconf/202022401038.

[26] Z. Ayop, C. Yee, S. Anawar, E. Hamid, and M. Syahrul, "Location-aware event attendance system using QR code and GPS technology," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 9, 2018, doi: 10.14569/IJACSA.2018.090959.

[27] B. D. Kumar and A. S. Kareemulla, "Smart mobile attendance system for employees using QR scanner," *Asian Journal of Applied Science and Technology (AJAST)*, vol. 1, no. 5, pp. 35–39, 2017.

BIOGRAPHIES OF AUTHORS

Muhammad Imanullah ⬤ 🔗 SC Ⓟ graduated from computer science of Brawijaya University, Indonesia, in 2016. He continued his study in Sepuluh Nopember Institute of Technology, Surabaya, and graduated in 2019. He currently works as a lecturer in Muhammadiyah University of Bengkulu. He has interest in the field of game technology. His research is connected to the field of human computer interaction, computer vision, and video games. Now he is focusing his career in academic and having dreams of digitizing some aspects in society related to cultural heritage as a preservation effort. He can be contacted at email: muhammad.iman@umb.ac.id.

Yuza Reswan ⬤ 🔗 SC Ⓟ has been researching in the field of image processing since graduated from Dian Nuswantoro University of Semarang, Indonesia, in 2012. He found his interest in the field since graduated from Dehasen University of Bengkulu, Indonesia in 2009. He currently works as a lecturer in Muhammadiyah University of Bengkulu. He can be contacted at email: yuzareswan@umb.ac.id.