Bima Journal of Science and Technology, Vol. 9(2A) Jun, 2025 ISSN: 2536-6041

DOI: 10.64290/bimagombe.v9i2A.1082

Two-Level Authentication IOT-Based Attendance Tracking System Using Fingerprint Biometry and RFID Card/Reader with Raspberry Controller

Alhassan Haruna Umar[1]*, Sa'id Musa Yarima[2], Amiru Ali[3] and Abdullahi Mohammed Ibrahim[4]

[1]Department of Computer Engineering Technology, College of Engineering Technology, Jigawa State Polytechnic Dutse.
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering and Engineering Technology, Abubakar Tafawa Balewa University, Bauchi.
[3,4]Department of Computer Science, College of Science and Technology, Jigawa State Polytechnic Dutse

Corresponding Author: ahumar@jigpoly.edu.ng

ABSTRACT

This paper proposes a secure and efficient attendance tracking system using a two-level authentication approach that combines fingerprint biometrics and RFID technology. The system utilizes a Raspberry Pi controller, a GT-521F52 fingerprint module, and an RFID tag/reader to capture and verify students' attendance. The fingerprint biometric data is stored in both local memory and a cloud server, while the RFID authentication system employs the RC4 cryptographic algorithm to encrypt students' card Unique Identifiers (UIDs). The system ensures accurate and secure attendance tracking, with all recorded data saved to a database for easy access. This research contributes to the development of reliable and efficient attendance systems, with potential applications in educational institutions and other organizations.

Keywords: attendance tracking system, two-level authentication, fingerprint biometry, RFID technology, RC4 cryptographic algorithm.

INTRODUCTION

Class enrolment at Jigawa State Polytechnic in Dutse has become a significant challenge for the institution with over 1000 students often found in a single course; a situation that is becoming increasingly difficult to manage. In this situation, manually signing attendance on a paper document is a challenging task as it easily distracts the students, encourages proxy signing, and is largely unreliable in keeping accurate records. A proposed solution to overcome the challenges mentioned involves an automated system that uses biometrics to track attendance, offering high accuracy and efficiency, while also bypassing the shortcomings of conventional approaches. In this study, we propose the use of fingerprint recognition sensor, GT-521F52 and a radio frequency identification (RFID) implemented with Raspberry Pi technology to monitor attendance based on two-level authentication while also enabling the lecturer to access the stored data via either their personal computer or Android phone. A passive RFID system with a low-power consuming card reader enhances or circumvents potential issues that may be associated with scarred, moist or dirty fingers or even signal interference. For enhanced student attendance data reliability and security, we would have our existing data sent to the Blynk proprietary server which can be accessed by the lecturer's (administrator's) Android phone using the Blynk Android app to leverage on the strength of the Internet of Things (IoT).

The remaining part of this paper is organized as follows: Section 2 discusses the pertinent literature related to the objective of the research, and Section 3 describes the methodology regarding how the physical hardware is arranged, the development of the algorithm, and the flowcharts. The results

DOI: 10.64290/bimagombe.v9i2A.1082

are presented in Section 4, generally relating to detection, error, and error margin while Section 5 concludes the paper.

LITERATURE REVIEW

Student attendance is a critical factor in measuring learning progress, evaluating academic engagement, and gauging students' dedication to learning. It is a widespread policy in many educational establishments that students must achieve a specified attendance milestone to be permitted for final examination. The standard traditional method being employed for tracking student attendance involves circulating a paper document among the students, seated in rows and columns, where each student is required to enter their names along with other information such as their registration number and signature (Ardebili *et al*., 2022; Sarker *et al.*, 2016). This conventional practice is counter-productive for several reasons such as being extremely inconvenient in large classes, particularly in Nigeria's current academic setting, where as many as 200 - 1000 are made to sit in a single class or hall per course. The aforementioned method distracts the students, often leading to noise and, more intolerable, the tendency for fraud due to proxies by colleagues. Moreover, tedious effort would be required in circumstances where the manual attendance is required to be stored on a database (Sutabri *et al.*, 2019).

Many researchers have proposed diverse methods using one or combinations of technologies to proffer solutions ranging from simple to complex ones. For instance, Yi (2023) presented a simple implementation of the standard fingerprint biometry attendance in the most basic form was implemented and the results made attendance more convenient, fast and standardized compared with the traditional methods of signing on students' behalf or punching cards, thereby improving the convenience and effectiveness of learning environment in the university. A major analysis and comprehensive study by Mankar *et al.* (2024) reviewed the field of biometric attendance systems focused on application for educational institutions by consideration of time efficiency, user satisfaction, and accuracy in attendance tracking, evaluating methods, methodologies, technologies and implementations. However, in both (Yi, 2023) and (Mankar *et al*., 2024), many of the challenges with unfolding approaches such as learning and predictions were not discussed. As observed in (Yi, 2023) and (Mankar *et al*., 2024), Singh (2024) only utilized the fingerprint recognition technology for data acquisition, preprocessing, feature extraction, and matching to mitigate challenges like data privacy and security with robust solution. While the technique achieved significant improvement in reducing time theft, the accuracy of the system heavily relies on the quality of the fingerprint, which is often affected by dirt, skin exudates or skin impairment.

In another study, Louragli *et al*. (2024) proposed an RFID-based attendance mechanism utilizing the student wristbands, as opposed to employing fingerprint biometric systems. The system employed sensors with RFID tags embedded in the student bracelets to acquire the human biological signature. The method incorporates a real-time database, Google technologies such as Firebase, React.js, and Tailwind, along with Arduino chips and sensors with authentication using RFID. Recently, Nowsath (2024) developed an IoT biometric attendance system using a nexus-based approach by employing automated data streamlining and software orchestration, which aimed at enhancing attendance management by leveraging biometric technology and mobile applications. The proposed biometric system is designed to recognize and authenticate individuals by examining the unique characteristics of the human body. Upon confirmation of the student attendance by fingerprint sensors, the

DOI: 10.64290/bimagombe.v9i2A.1082

required messages are sent to parents to reduce absenteeism and lateness in the school.

In a more advanced or complex system, two or more technologies including machine learning (ML) algorithms have been proposed (Renisha *et al*., 2024; Thaleeparambil *et al*., 2024). In (Renisha *et al*., 2024), face recognition and RFID technology with no fingerprint biometrics were employed to provide dual-mode authentication to enhance data accuracy and security. Though the employed concepts are the same, the application developed by (Renisha *et al*., 2024) was an online college bus attendance system whereby each student is provided with an RFID to improve the accuracy and security of the attendance records. The system integrates face recognition using the YOLOv8 model and an RFID module. In contrast, Thaleeparambil *et al*. (2024) integrated an RFID with ESP8266 Wi-Fi modules, solenoid locks, servo motors, PIR sensors and visual recognition technologies with ESP-32 CAM modules to develop an automated attendance system to enhance classroom security and precision. The Wi-Fi and visual recognition components enhance the system's functionalities, facilitating wireless connectivity, instantaneous data transfer, and validation of identities. The solenoid locks and servo motors ensure controlled access, responding to validated attendance records while the PIR sensors detect motion, contrasting between genuine presence and proximity.

Some monitoring systems are purely ML-based, as demonstrated by Sidik *et al.* (2024) and Ennajar and Bouarifi (2024). Sidik *et al.* (2024) utilized the waterfall model, significantly improving accuracy and efficiency by incorporating IoT for web-based oversight and data archival to Microsoft Excel. This system allows data backup through a web interface but lacks reliable management and monitoring capabilities. Additionally, Ennajar and Bouarifi (2024) developed an integrated transfer learning technique using InceptionV3 and NASNetMobile architectures with trained convolutional neural networks for fingerprint recognition, achieving a performance accuracy of 99.86% with InceptionV3. To address these shortcomings, there is a need for an intelligent automatic attendance system that mitigates the drawbacks of traditional attendance processes using a Convolutional Neural Network (CNN) algorithm ML approach.

MATERIALS AND METHODS

The components for the implementation of the proposed research are the Raspberry Pi 4, GT-521F52 fingerprint module, RFID tag and RFID reader, PC, Android phone, and IoT platform as shown in Figure 1. The work proposes the use of an Internet-of-Things (IoT) based biometric fingerprint system where the student's fingerprint biometrics are initially captured via a biometric scanner, with the data subsequently stored both in memory and on a cloud server. To circumvent any eventuality of interference, the attendance system further incorporates an RFID authentication system based on RC4 (Rivest Code4), which is a cryptographic algorithm that encrypts the students' card Unique Identifier (UID). Our proposed system is constructed around a Raspberry Pi Pico (or a Pi 400 or the 4th generation) employing a fingerprint sensor module of the GT511C3 or GT-521F52 type. All recorded data are saved onto the database within the blink server, a proprietary version, allowing the user to access it at any time.

The system is low-power consuming and can be powered from batteries or standalone solar sources. Figure 1 describes the system architecture and hardware design which includes the Raspberry Pi, fingerprint sensor, RFID reader and software components, namely, the Blynk app and attendance database. Firstly, the Blynk server was

DOI: 10.64290/bimagombe.v9i2A.1082

integrated with the Raspberry Pi by installing both the Blynk library on the pre-installed Raspbian OS to enable IoT based linkage while the RFID reader and the biometric sensor GT-521F52 were connected to the Raspberry Pi. Next, the Raspberry Pi was configured with the necessary libraries and tools for data processing, the biometric data acquisition algorithm to capture, pre-process, and enhance fingerprint images. Subsequently, the feature extraction algorithms for accurate fingerprint recognition were implemented. This includes the RFID data acquisition and implementation of the second level authentication to read and process data. The practical sessions for the implementation of the two-level biometric card identification system are described in Figure 2 to Figure 5 covering different implementation stages.

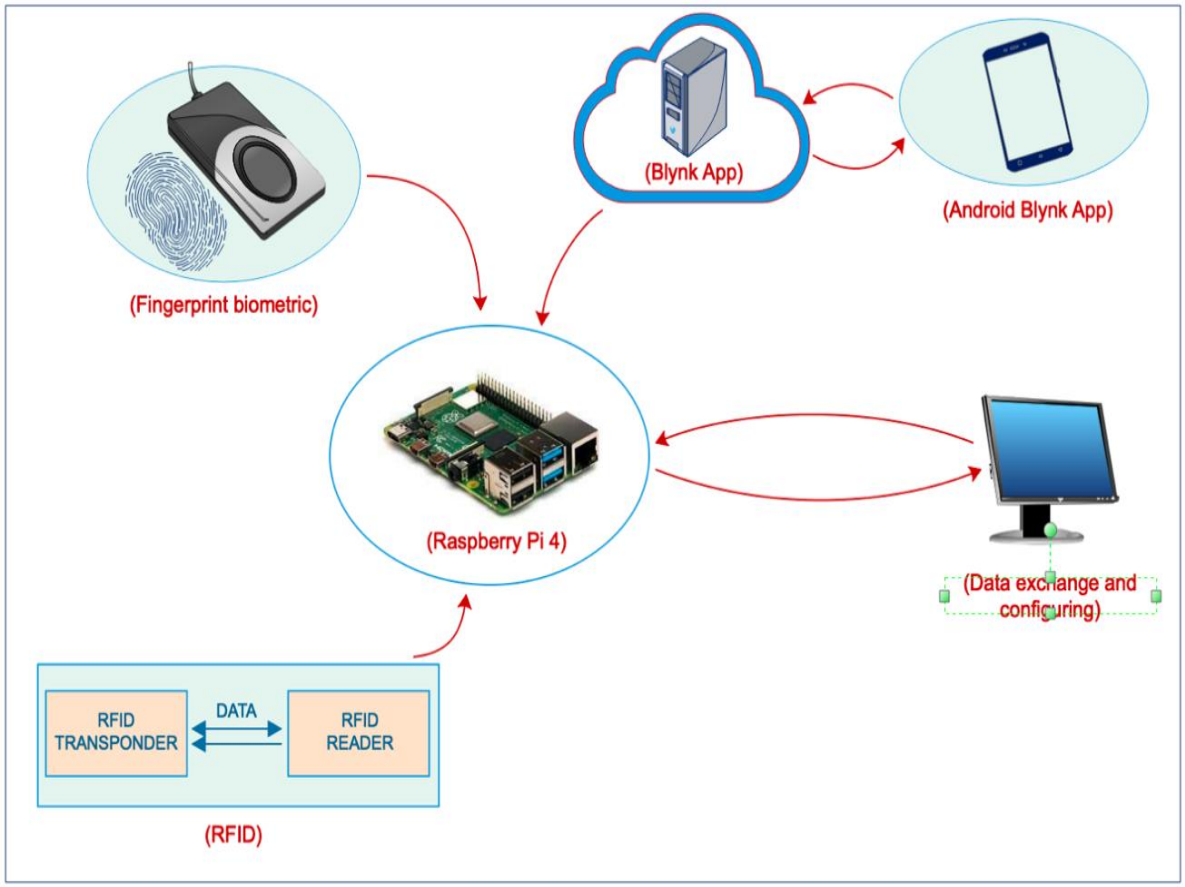

Figure 1: Smart student biometric attendance system with GT-521F52 fingerprint sensor and RFID.

To obtain the template ID of the GT-521F52 fingerprint module, the USB to TTL Serial Converter was used for the connection to the PC which converts the PC's USB signals to UART signals compatible with the GT-521F52. Jumper Wires (Female-Female or Male-Female) were used to connect the GT-521F52 pins (TX, RX, GND, VCC) to the USB to TTL serial converter and for easier wiring and prototyping, breadboard. The RC4 is used to encrypt and decrypt the challenge and response between the RFID tag and the reader. The shared secret key ensures that only authorized tags can respond correctly to the challenge, providing secure authentication.

Bima Journal of Science and Technology, Vol. 9(2A) Jun, 2025 ISSN: 2536-6041

DOI: 10.64290/bimagombe.v9i2A.1082

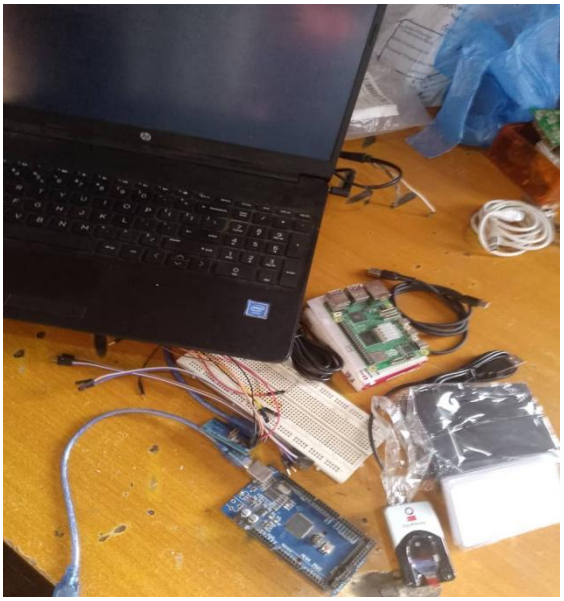

Figure 2: Initial set-up with all sensor elements, modules and PC.

Figure 3: Connections of GT-521F52 fingerprint module, RFID reader and tag around Raspberry Pi 4 microcontroller.

Figure 4: Testing the programmed Raspberry Pi 4 with the GT-521F52 fingerprint sensor module.

Figure 5: Testing the configured RFID card on the reader for RC4 authentication and functionality.

RESULTS AND DISCUSSION

Here we illustrate some results of our implementation of the detection algorithm designed around the row fingerprint template IDs and the validated IDs. The RFID authentication process works using RC4 as follows: In the RFID authentication process, the tag and the reader communicate when the RFID reader sends a request to the RFID tag to authenticate and the RFID tag responds with its unique identifier (ID). The RFID reader sends a random challenge to the RFID tag. The RFID tag uses RC4 to encrypt the challenge with a shared secret key. At this point, the RFID tag sends the encrypted response back to the RFID reader which the RFID reader uses the same shared secret key to verify the response by decrypting and verifying its authenticity. For the RC4 Encryption in RFID Authentication, the RFID tag and reader share a secret key and

Bima Journal of Science and Technology, Vol. 9(2A) Jun, 2025 ISSN: 2536-6041

DOI: 10.64290/bimagombe.v9i2A.1082

the RFID tag uses RC4 to encrypt the challenge with the shared secret key. The RC4 then generates a ciphertext from the challenge and shared secret key. For the verification, the RFID reader uses RC4 to decrypt the response with the shared secret key and if the decrypted response matches the original challenge, the RFID tag is authenticated successfully. The performance of the method was verified by the results in Figure 6 to Figure 9.

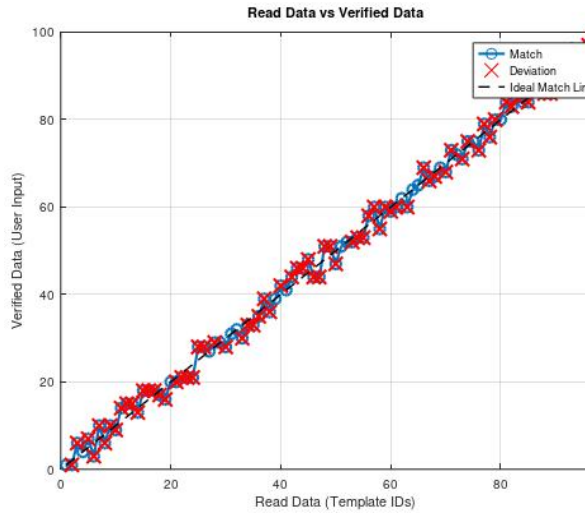

Figure 6: Template IDs obtain using USB to TTL Serial Converter with Raspberry Pi 4 to verify new fingerprints.

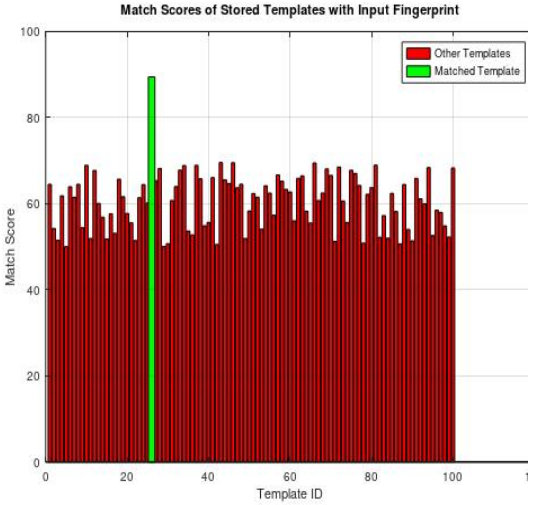

Figure 7: Evaluating match scores of stored templates with new fingerprints.

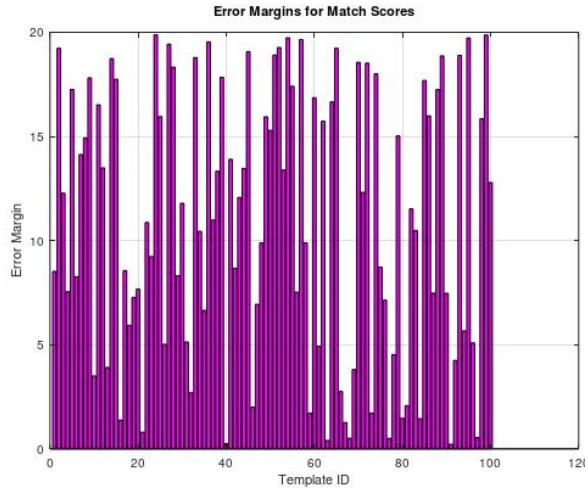

Figure 8: Margin of error with the recorded template IDs.

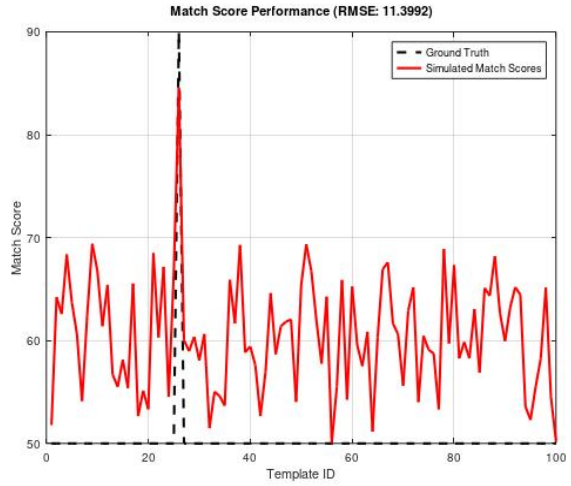

Figure 9: Evaluating the error mean of store and verified template IDs.

In Figure. 6, the fingerprint data template IDs were verified and authenticated by the RC4 algorithm while Figure 7 shows the match scores of the template ID with new fingerprint data. Figure. 8 represents the distribution for the margin of error while the performance based on the mean of squared error is shown in Figure 9.

CONCLUSION

A two-level authentication IoT-based student attendance system capable of acquiring fingerprint patterns has been successfully

DOI: 10.64290/bimagombe.v9i2A.1082

demonstrated. The system was tested to read, recognize and store fingerprint recognition using algorithms integrated with biometric authentication and a secured database to store biometric templates, RFID card data, and attendance records. The Blynk application was implemented with a user interface for the administrator (lecturer) and the communication between the Raspberry Pi and the Blynk server using the Blynk's IoT platform proceeds. Experimental results reveal the two-level fingerprint biometric module with RFID authentication works well within the predefined application environment of the class session. The attendance data can be shared between the module and the user's Android app via Blynk. Future improvement is expected to optimize the fingerprint patterns using the CNN ML algorithm to enable the system to accommodate a higher number of fingerprint inputs with accurate detection.

Acknowledgement

The authors would like to express their sincere gratitude to the Tertiary Education Trust Fund (TETFund) for the financial support through the 2024 institutional-based research intervention.

REFERENCES

Ardebili, A., Latifian, A., Aziz, C., BinSaeed, R., Alizadeh, S., and Kostyrin, E. (2022). A comprehensive and systematic literature review on the employee attendance management systems based on cloud computing. *Journal of Management & Organization, 1*(1), 1–18. https://doi.org/10.1017/jmo.2022.63

Ennajar, S., and Bouarifi, W. (2024). Enhancing student attendance system through fingerprint recognition using transfer learning techniques. *Proceedings of the 2024 International Symposium on Computer Vision (ISCV)*, 1–7. https://doi.org/10.1109/iscv60512.2024.10620112

Louragli, E. M., Gmih, Y., Soussi, S., and Farchi, A. (2024). Enhanced student attendance and communication in educational management systems. *Bulletin of Electrical Engineering and Informatics, 14*(1), 466–475. https://doi.org/10.11591/eei.v14i1.7915

Mankar, V., Jadhav, A., Golhar, G., Sambhe, P., Nitale, S., Kharode, B., Thakare, G., and Shriwas, M. K. (2024). Enhancing biometric attendance systems for educational institutions. *International Journal of Innovative Science and Research Technology.* https://doi.org/10.38124/ijisrt/ijisrt24mar2165

Nowsath, N. M. (2024). IoT biometric attendance system nexus with automated data streamlining and software orchestration. *Indian Scientific Journal of Research in Engineering and Management.* https://doi.org/10.55041/ijsrem29389

Renisha, P. S., Varghese, J., Jacob, N. M., Benny, F., George, R. Z., and Ahamed, R. (2024). Automated RFID and face recognition-based college bus attendance marking system with payment module. *Proceedings of the 2024 International Conference on Emerging Smart Technologies (ICTEST).* https://doi.org/10.1109/ictest60614.2024.10576119

Sarker, D. K., Hossain, N. I., and Jamil, I. A. (2016). Design and implementation of smart attendance management system using multiple step authentication. *2016 International Workshop on Computational Intelligence (IWCI)*, Dhaka, Bangladesh, 91–95. https://doi.org/10.1109/IWCI.2016.7860345

Sidik, A., Sunggono, N. T., Stianingsih, L., and Sidiq, Y. A. (2024). Utilization of Internet of Things (IoT) for biometrics attendance and web-based

DOI: 10.64290/bimagombe.v9i2A.1082

student monitoring. *Jurnal Sisfotek Global, 14*(2), 147–147. https://doi.org/10.38101/sisfotek.v14i2.15698

Singh, S. K. (2024). Biometric attendance system. *Indian Scientific Journal of Research in Engineering and Management, 8*(5), 1–5. https://doi.org/10.55041/ijsrem35127

Sutabri, T. S., Pamungkur, P., Kurniawan, A., and Saragih, R. E. S. (2019). Automatic attendance system for university students using face recognition based on deep learning. *International Journal of Machine Learning and Computing, 9*(5), 668–674.

Thaleeparambil, N., Biju, A., and Prathap, B. R. (2024). Integrated automated attendance system with RFID, Wi-Fi, and visual recognition technology for enhanced classroom security and precise monitoring. *Proceedings of the 2024 International Conference on Networking and Communications (INC)*, 4(1), 1–6. https://doi.org/10.1109/inc460750.2024.10649192

Yi, Y. (2023). Student attendance management system based on fingerprint identification technology. *Proceedings of the 2023 International Conference on Intelligent Information and Communication Systems (ICIICS)*, 1–5. https://doi.org/10.1109/iciics59993.2023.10420938.