JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

RFID BASED ATTENDANCE MANAGEMENT SYSTEM

[1]Dr. Dinesh Kumar D S, [2]Rakshith R, [3]Sharath M, [4]Shreyas P S Rao, [5]Uday C H

[1]Associate Professor, [2,3,4,5]Student
[1,2,3,4,5]Department of ECE
[1,2,3,4,5]KSIT, Bengaluru, India

Abstract : Maintaining the attendance of every individual in any organization like an educational institution or corporate workplace is an essential component. Traditionally, attendance systems relied on manual methods such as paper-based sign-in sheets or manual entry into spreadsheets, which were time-consuming, and prone to errors. Our prototype provides a practical approach to solving this problem with modern technology by using the method of Radio Frequency Identification (RFID) as it is a reliable, efficient, simple design, and low cost.

IndexTerms **- manual entry, Radio Frequency Identification (RFID), reliable, efficient, simple design, low cost.**

I. INTRODUCTION

The RFID based Attendance Management System represents an innovative approach to effectively managing attendance in various settings, such as schools, offices, and organizations. This system utilizes two key components: the RC522 RFID reader module and the EM-18 RFID reader module. The RC522 module is responsible for reading RFID tags, while the EM-18 module is designed specifically for reading RFID cards at a distance. By combining these modules, the Attendance Management System offers a seamless and reliable method for tracking attendance, enhancing efficiency, and eliminating manual processes.

With the RFID based Attendance Management System, users can effortlessly record attendance by simply swiping RFID cards within the range of the EM-18 module. Each RFID card or tag is unique to an individual, allowing for accurate identification and record-keeping. Additionally, the system can generate comprehensive reports, providing valuable insights into attendance patterns and trends. By automating the attendance management process, this system minimizes errors, saves time, and streamlines administrative tasks, ultimately contributing to a more efficient and productive environment.

II. LITERATURE SURVEY

Roberto Casula et al. [1] proposed the focus is on the vulnerability of modern fingerprint recognition systems to adversarial fingerprint presentation attacks. While these systems are generally accurate, artificial fingerprint replicas pose a significant threat, prompting the use of presentation attack detection (PAD) methods as a defense mechanism. Adversarial attacks, designed to manipulate fingerprint images and deceive PADs, were previously deemed theoretically unrealistic due to the need for internal system access. However, Casula proposes a novel method to generate robust adversarial perturbations that can withstand the physical crafting process of creating artificial fingerprint replicas. The introduction of a "focus attention" mechanism allows the concentration of perturbations on specific fingerprint regions. Experimental validation, including both white-box and black-box scenarios, illustrates the efficacy of the proposed method in generating realistic adversarial presentation attacks. The study emphasizes the potential threat posed by such attacks on fingerprint recognition systems, emphasizing the urgency of implementing protective measures.

Daniel Benalcazar et al. [2] focused on the adoption of remote biometric authentication for online services during the global pandemic of COVID-19. This allowed people to carry on with their normal business activities from home without the risk of spreading the virus. Some services include remotely opening a bank account, something that required physical attendance only a few years back. The downside of remote services is twofold. Firstly, in regions like South America, the accelerated technological Leap was too quick for some countries, resulting in difficulties for the national identification systems to catch up with the advancements, to properly increase the number of captured ID card image samples in our datasets for fraud detection using synthetic images, examples of the four classes must be generated: bonafide, composite, print and screen. This work presented four different methodologies capable of generating synthetic ID cards and evaluated the performance of each as a possible supplement for captured Images. For this purpose, we trained two MobileNetV2 networks using different combinations of captured and synthetic images, Further, obtaining real ID cards from new people and manually simulating composite, print, and screen attacks is very time-consuming and costly. Also, privacy regulations such as the GDPR assure individuals the right to withdraw their consent to use or store their private data, practically complicating the use and distribution of large datasets. Therefore, achieving similar performance with synthetic data and fewer resources is valuable for future applications and extension to other countries and improving the fake-ID detection techniques.

Nnamdi Henry Umelo et al. [3] proposed a groundbreaking solution to tackle the tag collision problem in dense Radio Frequency Identification (RFID) environments, such as those encountered on the Internet of Things (IoT). The proposed algorithm, named K-means grouped dynamic frame slotted Aloha (kg-DFSA), operates in two distinct stages. Firstly, in the initialization stage, tags are grouped using an

enhanced K-means clustering algorithm based on their unique RN16 codes, while a tag counter algorithm estimates the total number of tags. Subsequently, in the identification stage, tags respond to reader queries based on their group ID, minimizing collisions. The reader leverages the accurate tag estimate from the initialization stage to predict an optimal frame size, thereby reducing idle and collision slots while enhancing success slots and overall system efficiency. Simulation results demonstrate the superior performance of kg-DFSA in terms of system efficiency, success rate, and identification time, especially in dense RFID environments exceeding 500 tags. The algorithm's key strengths lie in its accurate tag estimation and optimal frame size selection, significantly enhancing RFID system performance for applications on the Internet of Things.

Zhiyuan He et al. [4] introduce PFVNet, a novel partial fingerprint verification network designed to address challenges in partial fingerprint matching. PFVNet integrates AlignNet, a spatial transformer network, to estimate affine transform parameters for effective image alignment, and CompareNet, a matching network with local self-attention, to classify genuine matches. The network is trained in a self-supervised manner using simulated partial fingerprint data, eliminating the need for time-consuming annotation. PFVNet outperforms other methods on datasets like FVC2006 DB1 and exhibits strong generalization across different scanners and image conditions. The network's visualization highlights its ability to automatically focus on multi-level fingerprint features, enabling effective matching of small and low-quality partial fingerprint images. Overall, PFVNet presents a robust solution for enhancing partial fingerprint verification.

Aditya Singh Rathore et al. [5] present Sonic Print, a novel fingerprint-based biometric identification method that capitalizes on the friction-excited sound waves produced when a user swipes their fingertip on a surface. Sonic Print utilizes the built-in smartphone microphone to capture and process the fingerprint-induced sound effect (FiSe), extracting multiple friction descriptors that encapsulate fingerprint information. An ensemble classifier achieves a commendable 98% identification accuracy in experiments involving 31 participants. Notably, Sonic Print proves resilient against various attacks, including fake fingers, replay attacks, and side-channel attacks, and exhibits potential for group authentication and object identification applications. Despite its promise, improvements are suggested to enhance reliability for users with damaged fingerprints and under adverse conditions, as well as the potential incorporation of more sensitive microphones for performance optimization.

Chengsheng Yuan et al. [6] focused on portable digital products such as smart phones, laptops, and unmanned vehicles, etc, trustworthy verification schemes in communication attract close attention from users. In the early stages, universal personal identity authentication broadly adopts passwords, token, PIN and cards, The inherent weakness, however, is that these schemes are easy to share, copy and clone, making it impossible to ensure that legitimate users are present. Secondly, employees may also make fingerprint moulds for themselves to deceive the fingerprint attendance machine (FAM). Hence, spoofing attacks become a huge challenge in AFIS, meanwhile, it is of great practical significance to identify whether the fingerprints to be tested are live or fake before identification using fingerprints. Most of them usually considered global pattern differences existed in fingerprint images and classified them via learning these pattern differences between live and fake fingerprints using deep learning methods. However, learning such a subtle minutia between them often contains large amounts of network parameters, inevitably consuming too much inference time. Studies have shown that many sweat holes are distributed on the mastoid stripes of live fingerprints, which have relatively stable shape, position, size, and density, and they are the source of sweat production. Fingerprint authentication technology has been broadly applied in daily life, but the emergence of spoofing attacks poses a great security threat to the current AFIS. In this paper, a fingerprint liveness detection method based on spatial ridge continuity has been proposed. The scheme proposed in this paper preliminarily considers the continuity within and between fingerprint slices and ignores the combination of more continuity features. We will continue our research from the perspective of vertical and horizontal continuity of fingerprints. Similarly, we will try more experimental parameters on network design to optimize the proposed scheme.

Fatma A. Hossam Eldein Mohamed et al. [7] focused on an innovative cancellable biometric recognition framework that incorporates a hybrid structure of deformation tools, primarily utilizing encryption techniques to enhance security and safeguard user confidentiality. The encryption key is securely stored to prevent unauthorized access, and RNA encryption lists, generated through Genetic Algorithms (GA), are employed for creating initial cipher images. The cancellable biometric system undergoes validation through extensive simulation experiments across diverse biometric databases, exhibiting promising results in terms of Area Under the Receiver Operating Characteristic (AROC) and False Acceptance Rate (FAR) values. The proposed hybrid RNA-GA encryption algorithm contributes to more uniform histograms for cancellable templates, demonstrating high correlation scores in genuine tests and low correlation scores in imposter tests. The research team, consisting of experts in antennas, wave propagation, data security, cryptography, and information technology management, underscores the multidisciplinary nature of the project. Overall, the framework presents a robust solution for biometric recognition, prioritizing security, and achieving favorable performance metrics in experimental validations.

Kyeongmin Park et al. [8] focused on a fingerprint-scanning analog front-end (AFE) designed for under-glass mutual-capacitive fingerprint sensors. These sensors considered more cost-effective and reliable for full screen displays than optical or ultrasonic alternatives, face challenges in thicker glass scenarios where capacitance variation between fingerprint ridges and valleys is reduced. External noise from the display and charger further impacts the AFE's signal-to-noise ratio when integrated into a display. The proposed solution employs a differential sensing structure, high-voltage transmitters, and a lock-in architecture, achieving a capacitance resolution of 17 at to farads and improving the signal-to-noise ratio to 13.4 dB at a 120 Hz frame rate. A differential phase-encoded sequential driving scheme and on-chip replica channel compensate for offset errors and enhance the dynamic range. Measurement results demonstrate noise immunity up to 500 kHz and a power consumption of 23.2 milliwatts, highlighting the AFE's capability to overcome challenges associated with thicker glass and external noise sources in under-glass mutual-capacitive fingerprint sensors.

Guochun Wan et al. [9] discussed on a novel detection method for chipless radio frequency identification (RFID) tags based on maximum likelihood estimation decoding. Chipless RFID tags encode data using notches in their frequency response spectrum. The proposed method uses a software defined radio platform to detect the power response of the RFID tags across a frequency band. Then, a maximum likelihood estimation decoding algorithm is used to identify the tag based on the entire power response curve, rather than just the presence or absence of notches. This approach is more robust to variations in notch amplitude and resonance frequency offsets compared to conventional threshold-based decoding methods. The text describes the design of a 6-bit chipless RFID tag using spiral resonator structures and an ultrawideband

antenna for detection. Experimental results demonstrate that the maximum likelihood estimation decoding algorithm can correctly identify the tags and is feasible for multilevel amplitude coding and mixed tag recognition with different coding methods. The software defined radio platform provides flexibility and feasibility compared to traditional network analyzer detection methods.

S. M. Anzar et al. [10] focused on the Random Interval Attendance Management System (RIAMS), a proposed system aimed at managing student attendance in virtual classrooms. RIAMS employs a face recognition module built with the Dlib software library to identify students based on facial features extracted from video frames during virtual classes. To enhance accuracy, the system utilizes CAPTCHAs and UIN queries at random intervals to verify student engagement, preventing predictability. The outputs from face recognition and ancillary modalities are combined using weighted sums, offering a reliable multimodal approach. RIAMS optimizes bandwidth usage by requiring students to activate their cameras for brief periods at random intervals. This innovative system ensures attendance monitoring and engagement checks in virtual learning environments, maintaining student focus without disrupting the learning process—particularly relevant in the context of the COVID-19 pandemic.

III. METHODOLOGY

The attendance management system operates seamlessly through a carefully orchestrated sequence of steps, leveraging RFID technology, fingerprint scanning, and real-time data synchronization with Google Sheets. The system begins by initiating the attendance process when the teacher's RFID card is scanned using the EM-18 reader module. This module reads the card's unique ID and transmits the data to the ESP8266 module, which serves as the central hub for data processing and communication. Upon receiving the teacher's RFID data, the ESP8266 module establishes a secure connection with the Google Sheets linked to the teacher's email ID. This connection enables real-time updates to attendance records, ensuring accuracy and efficiency in data management. With the groundwork laid, students proceed to confirm their attendance by scanning their RFID tags using designated scanners. Following the successful scanning of RFID tags, students verify their attendance by scanning their fingerprints. The fingerprint data is captured and transmitted to Google Sheets, where it is recorded alongside the corresponding RFID data. This dual verification process enhances the security and reliability of attendance tracking, minimizing the risk of fraudulent entries or errors. Throughout the attendance process, the system provides real-time feedback to users through an OLED screen and LED indicators. The OLED screen displays student details such as name and unique student number (USN), allowing for quick verification of attendance status. A blinking green LED confirms successful entry for each student, ensuring a seamless and efficient registration process. In the event of an invalid RFID tag being scanned, the system promptly alerts users with a blinking red LED and displays the message "Invalid ID" on the OLED screen. This immediate feedback allows for quick resolution of discrepancies and ensures the integrity of attendance data. Similarly, if an invalid teacher's RFID card is initially scanned, the system signals this with a blinking red LED and displays the message "Invalid card!" on the OLED screen, preventing further processing until a valid card is scanned. Additionally, the system incorporates safeguards to prevent errors or unauthorized access. In the rare scenario where two valid cards are scanned simultaneously, indicating a potential system glitch or attempted manipulation, all recorded student attendance data is automatically cancelled. Furthermore, updates to Google Sheets are temporarily halted to prevent any erroneous data entries. Finally, upon completion of the attendance process for all students, the teacher scans their RFID card to signify the end of the session. This action disables further student counts and triggers the display of the total student count on the OLED screen, providing a comprehensive summary of attendance for the session.

Table 3.1: Comparison of Various Fingerprint modules

Model	Capacity	Recognition time (in sec)	FRR (in %)
AD-013	40	< 0.6	6
GT-521F32	200	< 1.5	< 0.1
R307	1000	< 0.5	< 0.1

IV. BLOCK DIAGRAM

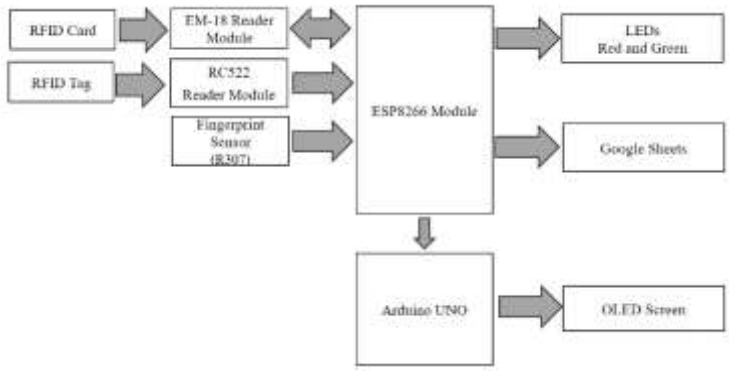

Fig 4.1: Block Diagram of the system

- RFID Card Reader Module (EM-18): This module reads the ID from an RFID card, such as a teacher's ID card. In the system you described, the EM-18 reader module transmits the teacher's ID data to the ESP8266 module.
- RFID Tag Reader Module (RC522): This module reads the ID from an RFID tag, such as a student's ID tag. In the system you described, the RC522 reader module likely transmits the student's ID data to the ESP8266 module as well.
- ESP8266 Module: This is the central processing unit (CPU) of the system. It receives data from the RFID reader modules, and likely performs tasks such as data validation and communication with Google Sheets.

- Fingerprint Sensor (R307): This sensor captures a fingerprint image from a user. In the system you described, the fingerprint sensor likely transmits the fingerprint data to the ESP8266 module.
- Arduino UNO (ATMEGA328P): This microcontroller is in serial communication with NodeMCU such that it instructs OLED to display the serial data from NodeMCU into the OLED Screen.
- OLED Screen: This screen displays information to the user, such as student names and messages. In the system you described, the OLED screen might show a student's name and ID number when their RFID tag is scanned successfully.
- LEDs (Red and Green): These LEDs provide visual cues to the user. In the system you described, a green LED might signal a successful student ID scan, while a red LED might signal an invalid ID scan.
- Google Sheets: This is a cloud-based spreadsheet application that stores the attendance data collected by the system. In the system you described, the ESP8266 module likely transmits the student ID data and fingerprint data to Google Sheets.

V. FLOW CHART

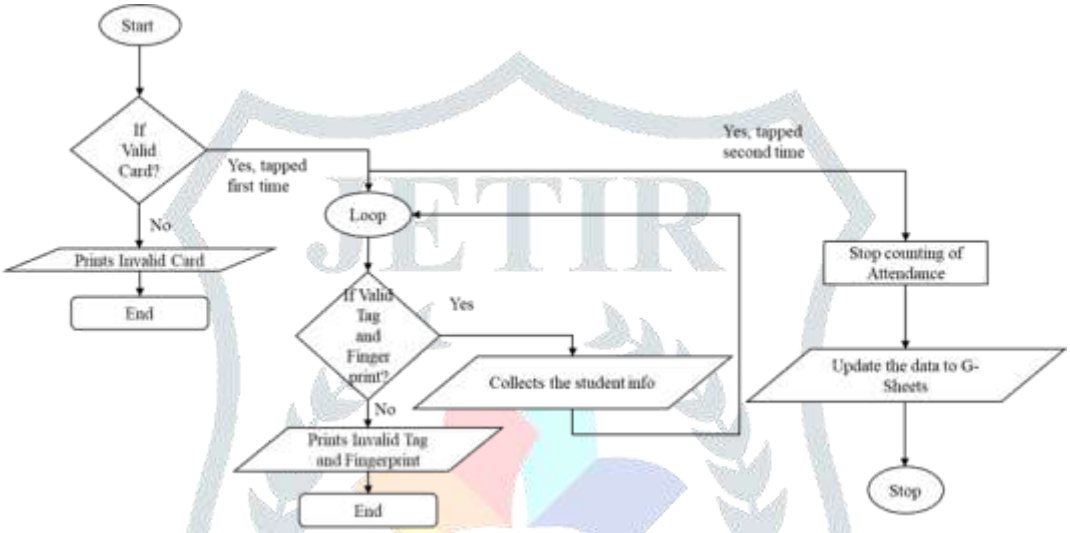

Fig 5.1: Flowchart of the system

The process of an attendance management system that leverages RFID tags, fingerprint verification, and Google Sheets for data storage.

Initiating Attendance Process

- Teacher Taps Card: The process commences with the teacher scanning their RFID card using the designated reader. The flowchart doesn't explicitly show this, but we can infer that the system first checks if this is the teacher's initial card scan.
- Validating Teacher Card: The system verifies the teacher's RFID card. If the card is invalid (meaning it's not recognized by the system), an "Invalid Card" message is displayed on the OLED screen, likely accompanied by a red LED signal (as referenced in the text description you provided). This step prevents unauthorized users from initiating the attendance process.
- Teacher Card Confirmed: If the teacher's card is valid, the system proceeds to the next stage, which involves recording student attendance.

Recording Student Attendance

- Student Scans RFID Tag: Students proceed to scan their RFID tags one by one at the designated reader.
- Validating Student ID: The system validates the scanned student ID. An invalid student ID could indicate a missing or damaged tag, or a student attempting to use another student's tag. The flowchart shows that if the student ID is invalid, an "Invalid Tag and Fingerprint" message is displayed, and the system stops recording attendance data, presumably to prevent errors.
- Fingerprint Verification: Once a valid student ID is scanned, the student verifies their attendance by placing their finger on the fingerprint sensor. The captured fingerprint data is compared against the student's fingerprint data stored in the system's database.
- Valid Fingerprint: If the fingerprint matches the student's data, the system marks the student's attendance as "present" in Google Sheets. The OLED screen likely displays the student's name and ID for confirmation, and a green LED might illuminate to signal successful registration.
- Invalid Fingerprint: If the fingerprint doesn't match the stored data, the system displays an "Invalid Tag and Fingerprint" message, similar to the scenario for an invalid student ID. Attendance recording is halted to prevent unauthorized attendance marking.

Ending Attendance Process

- Teacher Ends Session: After all students have scanned their ids, the teacher taps their card again to signify the end of the attendance session. The system recognizes this as the end point.

- Total Count Displayed: The system stops counting students and displays the total student attendance for that session on the OLED screen. This provides a quick summary for the teacher.

Additional Considerations

The flowchart doesn't explicitly show these, but the text description mentions a couple of additional features:

- Safeguards: The system incorporates safeguards to prevent errors or unauthorized access. For instance, if two valid teacher cards are scanned simultaneously, the system cancels all recorded student attendance data and halts updates to Google Sheets to prevent inconsistencies.
- Real-time Updates: The ESP8266 module likely establishes a connection with Google Sheets linked to the teacher's email ID, enabling real-time updates to attendance records. This ensures data accuracy and minimizes the risk of data loss.

VI. FUTURE SCOPE

The proposed system is further developed as follows:

- This system can be embedded into online video chat applications such as Zoom, MS Teams Webex, etc during online classes.
- This system can be further developed by implementing a face recognition system for effective two-stage verification.

VII. RESULT

Fig 7.1: Project Setup

The Attendance system is booted and is connected to Wi-Fi and G-Sheets. Green LED blinks once the NodeMCU is connected to Wi-Fi and is displayed on the OLED Screen.

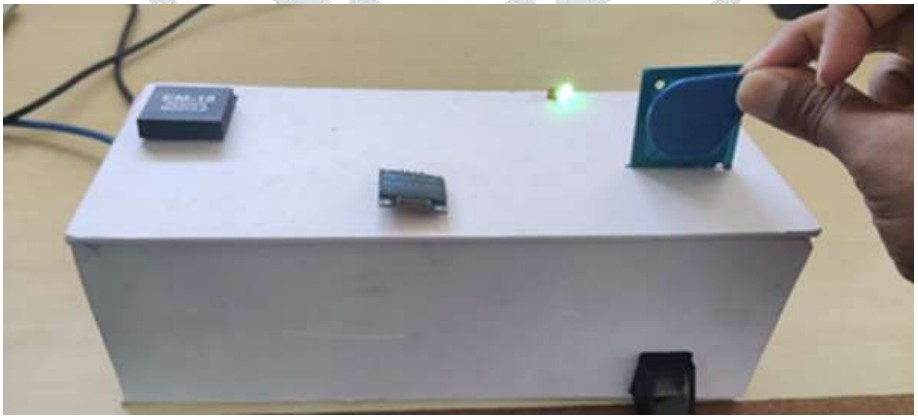

Fig 7.2: Valid Tag Verification

Once the device is set up and a valid RFID card held by the teacher is scanned for the first time, students scan their RFID Tag. Once a valid tag is scanned, student name and USN are displayed on the OLED screen and the Green LED blinks.

Fig 7.3: Finger ID verification

Once a valid tag is read, after a 2.5 sec delay, the student verifies his fingerprint. If the fingerprint matches, Green LED blinks and OLED displays "Verified".

Fig 7.4: Invalid Finger ID is detected

If an invalid fingerprint ID is detected, Red LED blinks and "Invalid Finger ID".

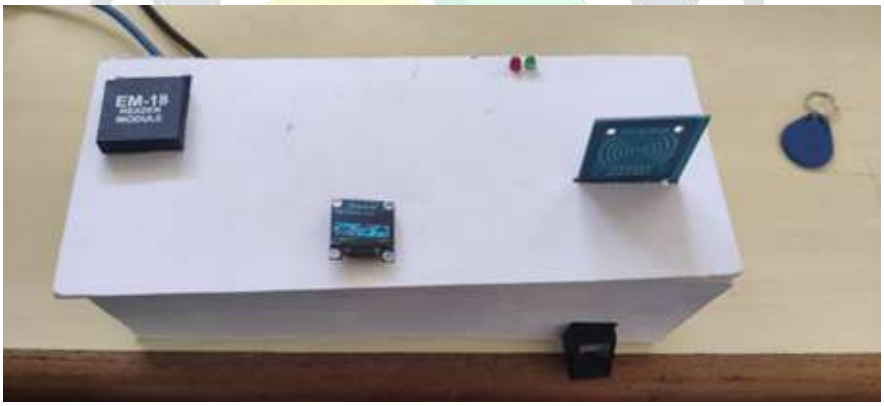

Fig 7.5: Publishing data to G-Sheets

Once all students have verified their attendance, the teacher scan the RFID card for the second time, all the collected data during the attendance is being updated to google sheets.

	A	B	C	D	E	F	G	H	I	J
1	Name	USN		15/04/2024	16/04/2024	17/04/2024	18/04/2024	19/04/2024	20/04/2024	22/04/2024
2	Rakshith R	1KS20EC077	0	0	1	2	3	4	5	5
3	Sharath M	1KS20EC093	0	1	2	2	3	4	4	4
4	Shreyas P S Rao	1KS20EC098	0	1	2	2	3	4	4	5
5	Uday C H	1KS20EC108	0	0	1	2	3	3	4	4

Fig 7.6: G-Sheets Updation

When the attendance data is sent to G-sheets by the NodeMCU, the student data is updated corresponding to the student identity.

If the student is present, His/her previous day attendance is added with the new attendance data.

If the student is absent, his/her previous day attendance is retained as it is.

VIII. Conclusion

In conclusion, the RFID-based attendance system with fingerprint verification, seamlessly integrated with the ESP8266 module, offers a cutting-edge solution to address the dynamic requirements of contemporary attendance management. This system combines RFID technology

for swift and accurate identification with an additional layer of security through fingerprint verification, ensuring the precision and reliability of attendance tracking. The integration of ESP8266 enhances the system's capabilities, enabling real-time data transmission for instant updates and attendance record monitoring. Beyond streamlining administrative processes, the system fosters accountability and transparency in educational institutions, businesses, and other organizations where attendance tracking is paramount. As technology progresses, solutions like this pave the way for more sophisticated and secure attendance management, contributing to a more efficient and organized operational environment.

IX. APPLICATIONS

- Educational institutions: The system can be used by schools, colleges, and universities to manage student attendance efficiently.
- Corporate offices: The system can be used by companies to manage employee attendance, monitor absenteeism, and generate attendance reports.
- Hospitals: The system can be used in hospitals to track the attendance of doctors, nurses, and other staff members.
- Government organizations: The system can be used by government organizations to track the attendance of employees and ensure accountability.
- Libraries: The system can be used in libraries to manage the attendance of librarians and track the usage of library resources.
- Fitness centers: The system can be used in fitness centers to manage the attendance of members, track the usage of facilities, and monitor the performance of trainers.

REFERENCES

[1] Roberto Casula, Giulia Orrù, Stefano Marrone, Umberto Gagliardini, Gian Luca Marcialis and Carlo Sansone, “Realistic Fingerprint Presentation Attacks Based on an Adversarial Approach”, IEEE transactions on information forensics and security, vol. 19, 2024.

[2] Daniel Benalcazar, Juan E. Tapia, Sebastian Gonzalez, and Christoph Busch, “Synthetic ID Card Image Generation for Improving Presentation Attack Detection”, IEEE transactions on information forensics and security, vol. 18, 2023.

[3] Nnamdi Henry Umelo, Nor Kamariah Noordin, Mohd Fadlee A. Rasid, Kim Geok Tan and Fazirulhisyam Hashim, “Efficient Tag Grouping RFID Anti-Collision Algorithm for Internet of Things Applications Based on Improved K-Means Clustering”, IEEE access volume 11, 2023.

[4] Zhiyuan He, Jun Zhang, Liaojun Pang, and Eryun Liu, “PFVNet: A Partial Fingerprint Verification Network Learned from Large Fingerprint Matching”, IEEE transactions on information forensics and security, vol. 17, 2022.

[5] Aditya Singh Rathore, Chenhan Xu, Weijin Zhu, Afee Daiyan, Kun Wang, Feng Lin, Kui Ren, and Wenyao Xu, “Scanning the Voice of Your Fingerprint with Everyday Surfaces”, IEEE transactions on mobile computing, vol. 21, no. 8, August 2022.

[6] Chengsheng Yuan, Peipeng Yu, Zhihua Xia, Xingming Sun, and Q. M. Jonathan Wu, “FLD-SRC: Fingerprint Liveness Detection for AFIS Based on Spatial Ridges Continuity”, IEEE journal of selected topics in signal processing, vol. 16, no. 4, June 2022.

[7] Fatma A. Hossam Eldein Mohamed, Walid El-Shafai, Hassan M. A. Elkamchouchi, Adel Elfahar, Abdulaziz Alarifi, Mohammed Amoon, Moustafa H. Aly, Fathi E. Abd El-Samie, Aman Singh, and Ahmed Elshafee, “A Cancelable Biometric Security Framework Based on RNA Encryption and Genetic Algorithms”, IEEE access volume 10, 2022.

[8] Kyeongmin Park, Seunghun Oh, Sanghyun Heo, Sangwoong Shin, and Franklin Bien, “17-aFrms Resolution Noise-Immune Fingerprint Scanning Analog Front-End for Under-Glass Mutual-Capacitive Fingerprint Sensors”, IEEE transactions on circuits and systems—I: regular papers, vol. 69, no. 3, March 2022.

[9] Guochun Wan, Mingxu Zhang, Wenzhao Li, and Lan Chen, “A Novel Detection Method Based on Maximum-Likelihood Estimation Decoding of a 6-bit Chipless Radio Frequency Identification Coded Tag”, IEEE transactions on instrumentation and measurement, vol. 70, 2021.

[10] S. M. Anzar, N. P. Subheesh, Alavikunhu Panthakkan, Shanid Malayil, and Hussain Al Ahmad, “Random Interval Attendance Management System (RIAMS): A Novel Multimodal Approach for Post-COVID Virtual Learning”, IEEE access volume 9, 2021.