IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International 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 Electronics and Communication Engineering,
[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.

***Index Terms* -** 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.

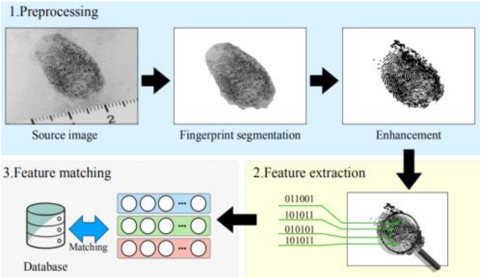

Figure 1: Schematic view of a ^{6}AFIS

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 favourable 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.

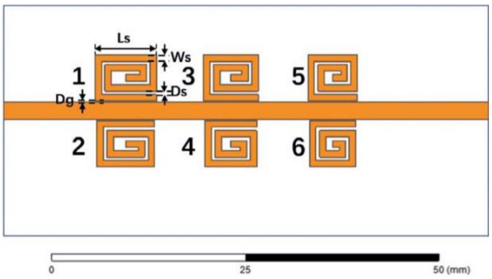

Figure 2: 6-bit chipless RFID Structure

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.

Chang Peng et al. [11] focused on a groundbreaking study on under-display ultrasonic fingerprint sensing for smartphones with narrow-bezel and full-screen displays. Existing fingerprint sensing techniques face challenges, but ultrasonic sensing, proven effective against spoof attacks, is explored. The first-ever multilayer under-display ultrasonic fingerprint sensor is theoretically designed and compared, with a lead zirconate titanate (PZT)-5A-based structure chosen. The fabricated sensor, operating at 20 MHz, exhibits a broad frequency response and high sensitivity suitable for under-display applications. Characterization and testing, including fingerprint-mimicking phantom imaging, demonstrate the sensor's potential. The study addresses the need for user-friendly front-side fingerprint recognition in modern smartphones and proposes an innovative solution to enhance security and usability.

Guoyi Xu et al. [12] introduce a prototype for indoor device-free object detection utilizing a Commercial Off-The-Shelf (COTS) RFID system. The proposed system employs a phase-based MF algorithm to assess the 3-D reflectivity distribution within the capture volume, providing comprehensive details on the system architecture and hardware components. Challenges such as localization accuracy, system, and computational cost are addressed, with a focus on a calibration technique to enhance accurate detection by eliminating extraneous factors. The system's performance is evaluated against local body movement and tag read rates, emphasizing the need to overcome these challenges for effective implementation. Additionally, the document provides supplementary materials and downloadable content, including a Digital Object Identifier (DOI) for reference (DOI: 10.1109/TIM.2021.3059309), making it a comprehensive exploration of the proposed RFID-based object detection system, covering algorithmic aspects, hardware details, challenges, calibration techniques, and performance evaluations.

Feng Liu et al. [13] propose a novel one-class fingerprint presentation attack detection method using an auto-encoder network. The method requires only real fingerprint samples for training, which helps improve its generalization ability. An auto-encoder is first trained only using bonafide fingerprint images. Then, the reconstruction error and latent code obtained from the trained auto-encoder are used as the basis for spoofness score calculation to detect presentation attacks. To achieve a more accurate reconstruction error, an activation map based weighting model is used to refine the reconstruction error. Different statistics and distance measures are calculated and finally fused using decision level fusion to make the final prediction. Experiments on a dataset with over 92,000 real fingerprints and 48,000 presentation attacks show that the proposed method achieves a true positive rate of 99.43% at a 10% false positive rate and 96.59% at a 5% false positive rate. This significantly outperforms existing feature based and supervised learning-based methods, demonstrating the effectiveness of the one-class auto-encoder based approach.

Abdulaziz Alarifi et al. [14] introduce an innovative optical PTFT asymmetric cryptography algorithm for the development of a secure and efficient cancel able biometric recognition system. Addressing the vulnerability of conventional biometric systems that store original biometrics, the proposed cancel able approach transforms biometric data into a different format to enhance security. Unlike most existing cancel able biometric methods that rely on symmetric encryption, this approach employs an asymmetric cryptography algorithm based on phase-truncated Fourier transform (PTFT). The PTFT algorithm utilizes two random phase masks as public encryption keys and two different random phase masks as private decryption keys, ensuring one-way encryption for improved security. Evaluation of diverse biometric datasets, including face, ear, palmprint, fingerprint, and iris images, demonstrates that the proposed system achieves higher accuracy and security compared to optical scanning holography and double random phase encoding approaches. The system exhibits lower equal error rates, false accept rates, and false reject rates, showcasing robustness against noise and various types of attacks. Overall, the proposed system emerges as a robust and secure solution for cancel able biometric authentication.

Yang Yu et al. [15] present a novel method for registering external and internal fingerprints acquired from distinct sensors, addressing the challenges posed by differences in image styles and deformations between the fingerprints. The authors introduce a cycle generative adversarial network with a structural constraint to enhance the similarity between internal and external fingerprints, effectively transferring the internal fingerprint's image style while preserving ridge-valley structures. A two-step registration process follows, involving fast digital image correlation with outlier rejection for coarse registration and denser sampling for fine registration, achieving global to local registration at subpixel accuracy. Comparative analyses demonstrate the superior registration accuracy and matching performance of the proposed method against other registration techniques. Ablation experiments underscore the effectiveness of individual modules within the proposed approach. Fusion results on the registered fingerprints reveal that, after precise registration, internal and external fingerprints can complement each other, providing more comprehensive fingerprint information for identification. In conclusion, the authors propose an efficient method for registering multisensor fingerprints obtained from diverse imaging systems, showcasing the potential of this approach in enhancing the quality of fingerprint information through registration and fusion.

Naeimeh Soltanieh et al. [16] provides a comprehensive review of radio frequency (RF) fingerprinting techniques used as an additional security layer for wireless devices. RF fingerprints, extracted from imperfections in analog components during manufacturing, serve to uniquely identify devices and prevent spoofing attacks. The review focuses on recent progress in RF fingerprinting methods, particularly transient-based approaches that analyze the transient part of the signal. Various transient extraction techniques are theoretically analyzed. The paper also explores methods using the modulated part of the signal. It covers applied methodologies, classification algorithms, and features taxonomy. The goal is to present a state-of-the-art overview of RF fingerprinting methods, addressing challenges, and discussing the practical deployment of low-end devices. The review concludes with a classification methodology for transmitter identification.

Grishma Khadka et al. [17] introduces a novel error correction technique for chipless RFID tags using punctured convolution coding (PCC). The chipless RFID system employs passive microwave resonators on a PCB, reflecting backscatter signals with unique frequency signatures for data encoding. The proposed PCC-based approach eliminates the need for an integrated circuit on the tag, handling error correction during the tag's design and fabrication process. The PCC-encoded chipless RFID tag is detected based on resonance frequencies resembling logic "1" and "0," and a Viterbi decoder is employed for error detection and recovery. The technique demonstrates feasibility in encoding high data bits within limited bandwidth and exhibits the potential for robust error correction in cluttered environments.

Wu Lei et al. [18] introduce a pioneering dynamic fingerprint segmentation method centered on fuzzy C-means clustering and genetic algorithms, with the overarching goal of enhancing the precision of fingerprint identification systems. The method is initiated by employing a range filter on the fingerprint image to enhance ridge structures, followed by dynamic pixel clustering using a modified fuzzy C-means algorithm and genetic algorithm. The enhancement includes introducing weight coefficients based on pixel gray values in the fuzzy C-means algorithm. Genetic algorithms are then employed to determine optimal clustering centers, with the clustering number dynamically determined based on a validity index. Subsequent morphological post-processing operations remove background noise, yielding the fingerprint foreground region. Experimental results demonstrate the superior segmentation accuracy of the proposed dynamic method compared to existing approaches, showcasing the smallest average error across multiple fingerprint datasets. However, it is noted that the method currently incurs higher computational time, suggesting a potential avenue for improvement in future iterations. In summary, the proposed method offers an effective dynamic fingerprint segmentation technique that significantly enhances the accuracy of fingerprint identification systems.

Metodi P. Yankov et al. [19] focused on Fingerprint recognition stands out as a widely adopted biometric method, prized for its exceptional performance and robust security. The affordability of fingerprint sensors has led to their integration into a growing array of devices, including mobile phones, personal computers, and smart cards. To facilitate cost-effectiveness and increased integration, there is a trend towards employing small sensors. Conventionally, fingerprint recognition relies on minutiae-based methods, particularly for full-print size sensors. However, such methods may underestimate individuality in the case of small sensors, failing to capture the full identification capabilities of algorithms not confined to minutiae matching. This paper explores the application of mutual information (MI) and entropy estimation to binarized fingerprint images, with a specific focus on small sensor acquisition systems. Entropy, serving as a lower bound for code length, offers an estimate of fingerprint individuality. The study demonstrates that texture-based generative models enable entropy-per-pixel estimation independent of sensor size, relying solely on the active area within the fingerprint sample. Consequently, the biometric performance of complexity-unconstrained fingerprint recognition algorithms becomes contingent on the overlapping area between probe and reference samples. Through estimates of MI on public databases, this paper suggests conservative texture-based MI estimates that imply sufficient capacity for the identification of extensive populations, even with sensors as small as a few thousand pixels.

Kai Cao et al. [20] highlight the significance of latent fingerprints in law enforcement, emphasizing their widespread use and the challenges posed by their poor quality compared to reference prints. The paper discusses the current state of latent fingerprint recognition, revealing the performance gap between reference prints and latent prints. The need for automated latent recognition is emphasized, and the authors propose a Convolutional Neural Network (ConvNet)-based system. The paper addresses issues in the current practice, such as repeatability, throughput, and bias, and presents contributions, including multiple templates for latent representation and the development of a complete latent AFIS based on ConvNets. The proposed system's performance is evaluated, demonstrating its superiority over existing methods on benchmark databases. The paper concludes with a comprehensive review of related literature and a detailed explanation of the preprocessing and feature extraction steps in the proposed latent recognition system.

III. Methodology

The system operates by continually monitoring date and time through the RTC DS3231 module, with the RC522 module specifically active during college hours. The process begins with the teacher scanning their RFID card at the EM-18 reader module, which reads the unique ID and transmits the data to the ESP8266. The ESP8266 then connects to the Google Sheets linked to the teacher's email ID. Subsequently, students can scan their RFID tags to confirm their attendance, followed by fingerprint verification, with the data being sent to Google Sheets. The OLED screen displays student details, including name and USN, accompanied by a blinking green LED to confirm entry. In the event of an invalid tag, the red LED blinks, and "Invalid ID" is displayed on the OLED screen. Once all students have completed the process, the teacher scans their RFID card, disabling further student counts, and the OLED screen shows the total count. If an invalid card is initially scanned, the red LED blinks, and "Invalid card!" is displayed on the OLED screen. For extra classes, a button must be pressed within 10 minutes of college ending time to register attendance for an additional hour.

Table 1: Comparison of Various Fingerprint modules

Model	Capacity	Recognition time (in sec)	^{7}FRR (in %)
AD-013	40	< 0.6	6
GT-521F32	200	< 1.5	< 0.1
R307	1000	< 0.5	< 0.1

IV. Block Diagram

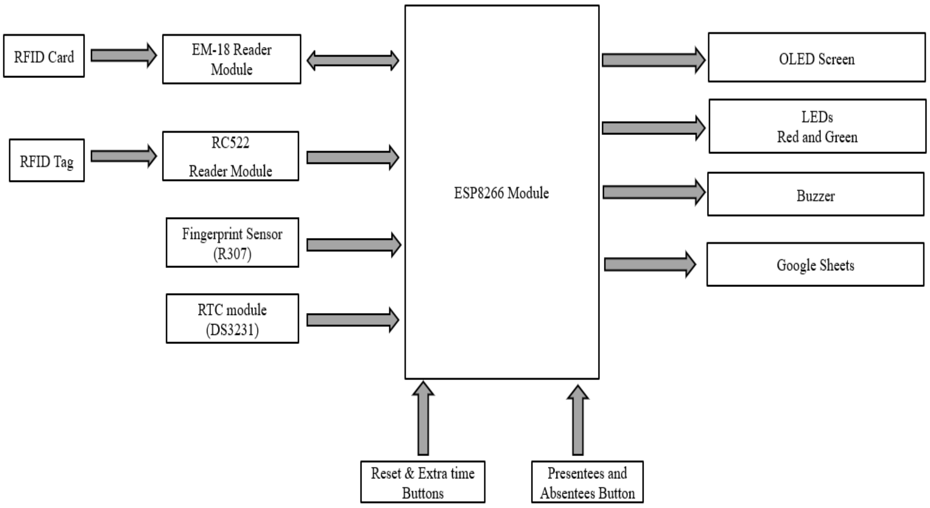

Figure 3: Block Diagram of the proposed system

V. 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.

VI. 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.

VII. 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.

VIII. Appendix

[6]AFIS – Automatic Fingerprint Identification System
[7]FRR – False Rejection Rate

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.

[11] Chang Peng, Mengyue Chen, Hongchao Wang, Jian Shen, and Xiaoning Jiang, "Broadband Piezoelectric Transducers for Under-Display Ultrasonic Fingerprint Sensing Applications", IEEE transactions on industrial electronics, vol. 68, no. 5, May 2021.

[12] Guoyi Xu, Pragya Sharma, Xiaonan Hui, and Edwin C. Kan, "3-D Indoor Device-Free Object Detection by Passive Radio Frequency Identification", IEEE transactions on instrumentation and measurement, vol. 70, 2021.

[13] Feng Liu, Haozhe Liu, Wentian Zhang, Guojie Liu, and Linlin Shen, "One-Class Fingerprint Presentation Attack Detection Using Auto-Encoder Network", IEEE transactions on image processing, vol. 30, 2021.

[14] Abdulaziz Alarifi, Mohammed Amoon, Moustafa H. Aly, and Walid El-Shafai, "Optical PTFT Asymmetric Cryptosystem-Based Secure and Efficient Cancelable Biometric Recognition System", IEEE access volume 8, 2020.

[15] Yang Yu, Haixia Wang, Peng Chen, Yilong Zhang, Zhenhua Guo, and Ronghua Liang, "A New Approach to External and Internal Fingerprint Registration with Multisensor Difference Minimization", IEEE transactions on biometrics, behavior, and identity science, vol. 2, no. 4, October 2020.

[16] Naeimeh Soltanieh, Yaser Norouzi, Yang Yang, and Nemai Chandra Karmakar, "A Review of Radio Frequency Fingerprinting Techniques", IEEE journal of radio frequency identification, vol. 4, no. 3, September 2020.

[17] Grishma Khadka, Md Shamsul Arefin, and Nemai Chandra Karmakar, "Using Punctured Convolution Coding (PCC) for Error Correction in Chipless RFID Tag Measurement", IEEE microwave and wireless components letters, vol. 30, no. 7, July 2020.

[18] Wu Lei and You Lin, "A Novel Dynamic Fingerprint Segmentation Method Based on Fuzzy C-Means and Genetic Algorithm", IEEE access volume 8, 2020.

[19] Metodi P. Yankov, Martin A. Olsen, Mikkel B. Stegmann, Søren Sk. Christensen, and Søren Forchhammer, "Fingerprint Entropy and Identification Capacity Estimation Based on Pixel-Level Generative Modelling", IEEE transactions on information forensics and security, vol. 15, 2020.

[20] Kai Cao and Anil K. Jain, "Automated Latent Fingerprint Recognition", IEEE transactions on pattern analysis and machine intelligence, vol. 41, no. 4, April 2019.