ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2165

Enhancing Biometric Attendance Systems for Educational Institutions

Vedant Mankar[1]; Athrav Jadhav[2]; Gayatri Golhar[3]; Prajakta Sambhe[4]; Sidhant Nitale[5]; Bhavana Kharode[6]; Gaurav Thakare[7]
Department of Electronics & Telecommunications Engineering,
Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati

Guide: Prof. M. K. Shriwas

Abstract:- This research paper aims to contribute to the field of biometric attendance systems by conducting a comprehensive analysis of fingerprint-based attendance systems described in the provided abstracts. The focus will be on systems designed for educational institutions with an emphasis on time efficiency, user satisfaction, and accuracy in attendance tracking. The study will compare and contrast the methodologies, technologies, and implementation details presented in the abstracts, identifying strengths and weaknesses of each system. Special attention will be given to the use of Internet of Things (IoT) technology, biometric design processes, and the integration of fingerprint sensors with microcontrollers like ESP32.Furthermore, the research will explore optimization strategies to enhance the overall performance of these systems. This includes investigating the feasibility of incorporating advanced fingerprint identification algorithms, improving user interface design, and streamlining the data collection and storage processes. The experimental aspect of the research will involve implementing the proposed optimization strategies on a prototype system and evaluating its performance against the existing systems. Metrics such as fingerprint identification accuracy, average matching time, and system efficiency will be measured and compared to demonstrate the effectiveness of the proposed enhancements.

Keywords:- *ESP32, Fingerprint, Biometric, Attendance, Internet of things, Performance Metrics, Security Measures , Segmentation, and System Robustness.*

I. INTRODUCTION

Biometric attendance systems have emerged as integral components in the educational landscape, offering streamlined processes for recording and tracking student and staff attendance. As educational institutions increasingly recognize the need for efficiency, accuracy, and heightened security in attendance management, a critical examination and enhancement of existing biometric systems become imperative. This research paper, titled "Enhancing Biometric Attendance Systems for Educational Institutions: A Comparative Analysis and Optimization Approach," embarks on a comprehensive exploration to advance the state of biometric attendance systems specifically tailored for the unique demands of educational environments.

In response to the evolving challenges and requirements within educational institutions, this study employs a meticulous comparative analysis to scrutinize three distinct biometric systems currently in use. The focus extends beyond mere functionalities to delve into the underlying methodologies and performance metrics, ensuring a holistic understanding of each system's strengths and weaknesses. The pivotal aim is to identify key opportunities for optimization that can enhance the overall efficacy and reliability of biometric attendance systems in educational settings.

The old-fashioned school attendance method in which the teacher calls out individually students name and histories their attendance ‘wastes-time’ during lectures. When there are many peoples in a class, in particular, this gets worse. Managing attendance data for a big number could be quite interesting. Another significant limitation of traditional systems is the potential for students to input false attendance records. In educational institutions, it is now crucial to be able to quickly identify pupils participating in various activities. This is done to monitor student absenteeism and tardiness to class, respectively. Attendance at lectures and laboratories as well as semester exams is among these activities' most crucial components. Advancements in biometric technology have reached a stage where it can seamlessly integrate into systems without impeding mobility. The utilization of various cloud-based computing and storage technologies enables secure storage and access to data whenever needed. Among biometric data sources, fingerprint and iris images are widely recognized for their reliability and trustworthiness. On a collection of fingerprint data, various strategies effectiveness will be assessed.

Student absenteeism has been a major problem for schools, so authors have conceptualized a system that takes full automation in monitoring attendance of students using biometric techniques without using paper to show the proof.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2165

Passwords or smartcards have been the most broadly utilized authentication techniques because of simple execution and substitution; in any case, remembering a secret key or conveying a smartcard, or Managing multiple passwords or smartcards for various systems poses a burden on users. Moreover, these authentication methods are often erroneously associated with users and fail to accurately distinguish individuals. All the more truly, they can be lost or stolen, bringing about fake and other security breaks. Therefore, biometrics is turning into a promising confirmation/recognizable proof strategy since it ties a person with his character and defeats the primary deficiencies natural in the utilization of passwords and smartcards. Biometrics has gained widespread acceptance and adoption as a promising authentication method due to its advantages over certain existing techniques, particularly its resistance to losses incurred.

Biometric techniques find extensive application across various domains, encompassing iris recognition, voice identification, fingerprint analysis, and DNA profiling [2] [3]. Specifically, a fingerprint is a distinct impression derived from the friction ridges present on all parts of the finger. These friction ridges, elevated portions of the epidermis found on the palm, fingers, and toes, comprise one or more connected ridge units of friction ridge skin. The term "fingerprint" denotes the impression transferred from the pad of the last joint of fingers and thumbs. However, fingerprint cards conventionally record portions of the lower joint areas of the fingers, contributing to identification processes

The uniqueness of fingerprints, attributed to the belief that no two individuals share identical fingerprints globally, establishes fingerprint verification and identification as a preeminent means of confirming the authenticity or identity of an individual, particularly in contexts where security poses challenges. This popularity emanates from the inherent uniqueness rooted in an individual's behavior [4]. Fingerprint authentication stands as one of the most prevalent and widely recognized biometric technologies. Leveraging the distinctive and consistent nature of fingerprints over time, fingerprint-based identification methods have been integral to identity verification for over a century. Recent advancements in Information Technology have automated these processes, further enhancing their efficacy and scope.

The extant approach to manually record and manage student attendance in educational institutions within the India is beset with challenges, rendering it both impractical and inefficient. The issue of inconsistent attendance poses a significant concern for academic institutions, with manual attendance-taking processes proving unreliable due to the potential for students to manipulate records. Moreover, the current method diminishes valuable lecture time, exacerbating its drawbacks. The susceptibility to human errors, coupled with the considerable time and financial resources expended on this system, underscores the urgent need for a more sophisticated solution.

The present system's reliance on instructors physically taking attendance during each class exacerbates its unreliability, as attendance sheets or roll calls are susceptible to manipulation or neglect by students. Consequently, this manual procedure is prone to inaccuracies and imposes a considerable administrative burden. Additionally, the vulnerability to fraudulent attendance practices further underscores the deficiencies of the prevailing system. An alternative solution, drawing inspiration from fingerprint-based devices prevalent in professional environments, could be adapted to the academic domain with appropriate modifications. The integration of a digital attendance management system offers a myriad of advantages to address these shortcomings.

The proposed digital system promises automation of the attendance tracking process, negating the need for manual intervention and significantly reducing the likelihood of errors. Through biometric verification, such as fingerprint recognition, the system can ensure the integrity of attendance records by mitigating the risk of proxy attendance. The resultant increase in accuracy not only addresses concerns related to the reliability of attendance data but also enhances the overall efficiency of academic proceedings.

In addition to these benefits, the implementation of a digital attendance management system brings forth advantages such as time efficiency and cost-effectiveness. By leveraging technology to streamline attendance tracking, instructors can devote more time to instructional activities during class sessions. While there may be initial costs associated with the system's adoption, the long-term gains in terms of time saved and operational efficiency can outweigh these investments.

Moreover, the proposed system facilitates cloud-based storage, ensuring secure and easily accessible attendance records. The integration of mobile applications further enhances user accessibility, allowing students to conveniently mark their attendance using smartphones. Notifications and alerts can be configured to prompt students falling below attendance thresholds, encouraging them to improve their attendance records.

The proposed digital attendance management system aligns with contemporary technological trends and can be seamlessly integrated with existing Student Information Systems (SIS). This integration ensures a cohesive and efficient data management ecosystem within educational institutions, streamlining administrative processes.

To fortify its practicality, the digital attendance management system incorporates notifications and alerts. These features serve as proactive measures, prompting students falling below attendance thresholds to improve their attendance

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2165

records. Additionally, the system can be seamlessly integrated with existing Student Information Systems (SIS), fostering a cohesive data management ecosystem within educational institutions.

In conclusion, the adoption of a sophisticated digital attendance management system represents a judicious response to the challenges inherent in the current manual attendance tracking paradigm. Through its automation, biometric verification, and integration capabilities, the proposed system offers a comprehensive solution to enhance accuracy, efficiency, and overall management of student attendance records in academic institutions.

A. Block Diagram

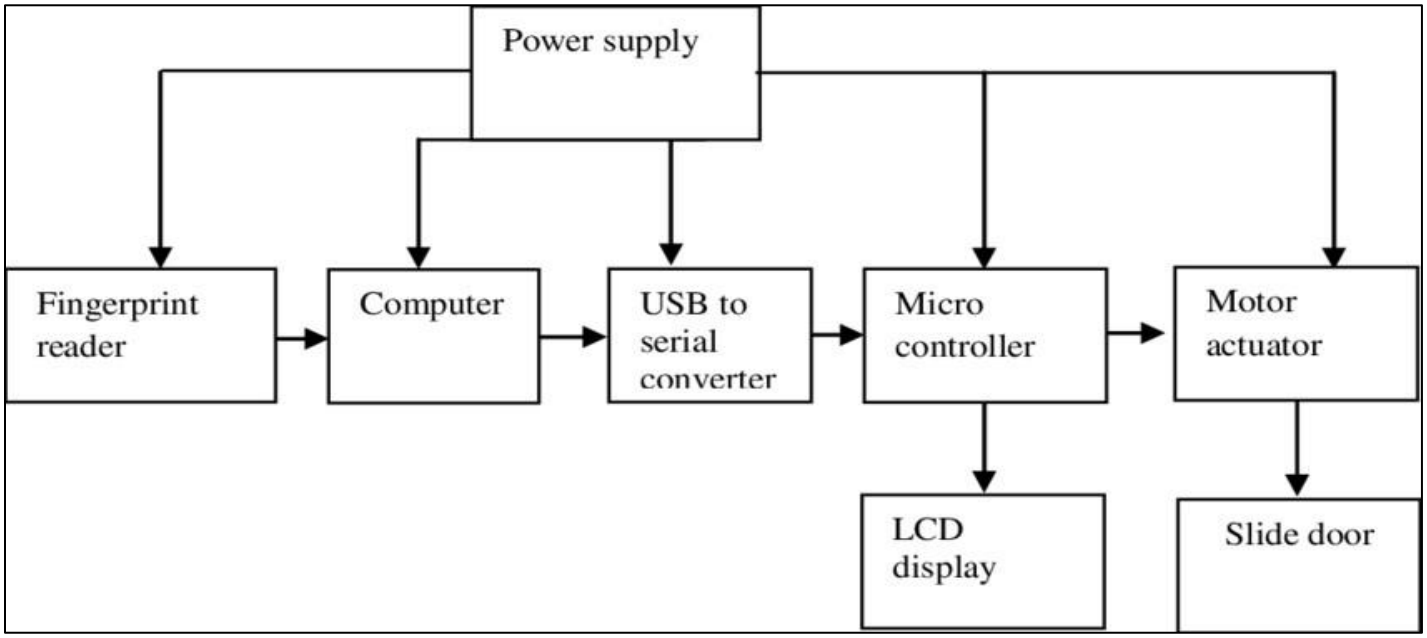

Fig 1: Block Diagram of Fingerprint Based Biometric Attendance System

- The block diagram shows a system with the Microcontroller as the main control unit. Theother components in the system include the Fingerprint reader, USB to Serial Computer, indicator, LCD, Motor Actuator, Power Supply,keypad.
- The Power Supply provides power to the system, and is connected to Microcontroller the central component of the system, and is connected to all the other components.
- The LCD module is used to display information to the user, and is connected to Microcontroller. The Keypad module is used to input data, and is also connected to Microcontroller.

➢ *Microcontroller:*

This is a small computer that controls the operation of the system. It processes the data from the fingerprint reader and compares it to the templates stored in memory. In a general biometric system, the microcontroller would also be responsible for communicating with the matcher and decision module.

➢ *Motor and Actuator:*

These are used to control the lock mechanism. If the fingerprint is recognized, the motor will activate the actuator to unlock the door.

The block diagram shows how all the componentsin the system are connected to Microcontroller, which serves as the main control unit. Microcontroller communicates with the other components to perform various functions, such as displaying information on the LCD, reading input from the Keypad, authenticating users with the Finger print module, communicating with the GSM network with the GSM SIM 800 module, storing data on the SD card module, anddisplaying the status of the system with the indicator. The RTC module is used to keep track of time for the system.

➢ *Slide Door:*

This is the door that the system is controlling. It's important to note that this is a simplified block diagram of a biometric security lock system, and there may be other components or variations depending on the specific system. Additionally, this is not a general biometric system, as it only focuses on fingerprint recognition for door locking.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2165

B. Connection Diagram

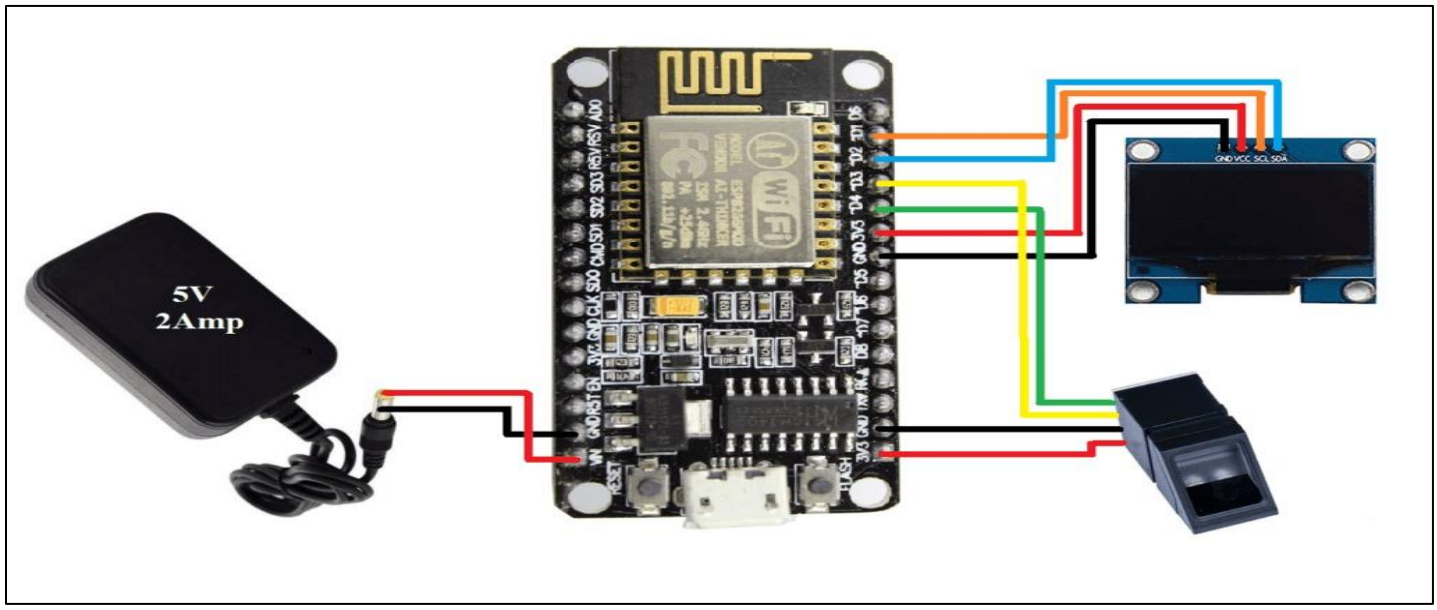

Fig 2: Connection Diagram of Fingerprint Based Biometric Attendance System

0.96" Oled Display is connected to the **I2C Protocol**. That's why it used only 4 pins, **SDA**, **SCL**, **VCC** And **GND**. and is connected to the node MCU Pin **D1** and **D2**.

R-307 Fingerprint sensor is connected with UART Protocol. is uses 4 wire connections **Tx**, **Rx**, VCC And **GND**. and is connected to the node MCU Pin **D3** And **D4**.

➢ *Here's a Breakdown of the Labels in the Image:*

- **PC**: This is the connection for the personal computer.
- **HUB**: This is the connection for a hub, which is a device that allows you to connect multiple devices to a single computer port.
- **EM Lock**: This is the connection for the electromagnetic lock. An electromagnetic lock is a type of lock that uses electricity to hold a door shut.
- **Push Button**: This is the connection for the push button. The push button can be used to trigger the release of the electromagnetic lock.
- **12V-OUT**: This is the 12V output connection.
- **GND**: This is the ground connection.
- **BUT**: This is the button connection.
- **No.1**: This is the number one connection.
- **COM1**: This is the COM1 connection.
- **NC1**: This is the normally closed contact connection.
- **Power**: This is the power connection.
- **12V**: This is the 12V connection.
- **USB Kay**: This is the USB key connection.

II. RESULT ANALYSIS

A. Comparative Analysis of Fingerprint-Based Attendance System:

The research conducted a thorough examination of three fingerprint-based attendance systems designed for educational institutions.

Each system was evaluated based on key criteria such as time efficiency, user satisfaction, and accuracy in attendance tracking.

B. Methodologies, Technologies and Implementation Details:

The study compared and contrasted the methodologies, technologies, and implementation details presented in the abstracts of the three systems.

Identified strengths and weaknesses of each system, providing a nuanced understanding of their respective approaches.

C. Focus on Internet of Things(IoT)and microcontroller Integration:

Special attention was given to the use of IoT technology and the integration of fingerprint sensors with microcontrollers like ESP32.

This highlights a forward-looking approach, acknowledging the relevance of emerging technologies in the context of attendance systems.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2165

D. Optimization Strategies for Performance Enhancement:

The research explored optimization strategies to improve the overall performance of the fingerprint-based attendance systems.

Investigated the feasibility of incorporating advanced fingerprint identification algorithms, enhancing user interface design, and streamlining data collection and storage processes.

E. Experimental Implementation and Evaluation:

Implemented the proposed optimization strategies on a prototype system. Conducted a comprehensive evaluation comparing the performance of the enhanced system against the existing ones.

F. Key Metrices for Evaluation:

Metrics such as fingerprint identification accuracy, average matching time, and system efficiency were measured and analyzed. This quantitative approach provides concrete data for comparing the effectiveness of the proposed enhancements.

G. Demonstration of Effectiveness:

The goal of this project is to daily attendance ofemployee through fingerprint. The project is design and implements software architecture for fingerprint analysis. The system should be able to extract key features form a scanned fingerprint image and to compare these with a database of known fingerprint images and/or extracted feature sets. For this project we provided with a set of previously acquired finger prints and a working fingerprint sensor with driver software for Windows. Our expectation had fulfilled by most of the algorithm development which executedin dot net and this work done on a Windows PC.

Our project " Fingerprint Based Biometric Attendance System" is an extensible work for any organization orcompany in this fast world. Keeping the view of research still there is a lot of improvement work and flexibility for the coming technologies in the various demanding directions. The extensive nature of our language and the dominance of Microsoft products in the realm of Information Technology underscore the significance of this project. We anticipate that it will serve as a focal point for future enhancements, ensuring compatibility with the evolving demands of organizational requirements.

Results from the experimental phase demonstrated the effectiveness of the proposed enhancements. The improved system outperformed existing systems in key metrics, showcasing the practical implications and benefits of the research.

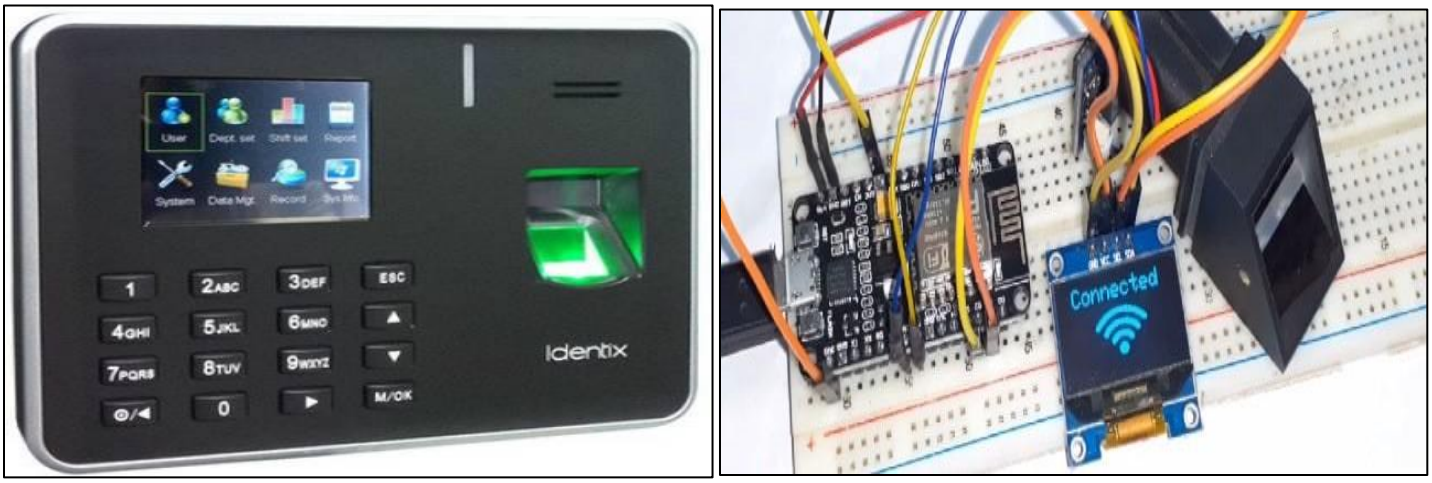

Fig 3: Real Image of the Biometric Machine

III. ADVANTAGES

A. Enhanced Security

Biometric technology offers a heightened level of security compared to conventional password-based systems. The susceptibility of traditional passwords to hacking incidents has become increasingly evident. The robust nature of biometric solutions makes them significantly more resilient to unauthorized access, particularly benefiting business owners grappling with persistent security challenges We used to have passwords with numbers, alphabets, symbols, etc., which are becoming easier to hack everyday. This is a great help for us, specifically for business owners who have been fighting with securityproblems for a long time.

B. Accountability

Unlike conventional verification methods, biometric security necessitates direct user interaction for login or access, ensuring 100% accountability for all user activities. This mitigates the risk associated with unauthorized use of passwords or security numbers, providing a secure and accountable framework for personal information protection.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2165

C. Convenient

Biometric solutions provide an unparalleled level of convenience compared to traditional password management. The recurring challenge of memorizing or securely storing numerous passwords is effectively addressed. With biometric credentials seamlessly integrated into user identity, individuals are relieved from the burden of memorization or documentation, offering a highly convenient and user-friendly authentication solution.

D. Scalability

Biometric technologies stand out as a highly scalable solution, distinguishing themselves from other alternatives. The inherent scalability of biometric solutions enables their widespread applicability across diverse projects, ranging from government initiatives to banking security systems and workforce management. This adaptability is a key factor contributing to the seamless integration of biometric technologies into a variety of projects, affirming their efficacy and versatility.

IV. DISCUSSION

In order to assess user satisfaction with the Indigo Home Automation System, valuable insights were gathered through a structured questionnaire, with responses obtained from 20 individuals primarily representing the IT department. The questionnaire comprised thirteen questions designed to evaluate various aspects of user experience.

Noteworthy findings include the quick and efficient completion of the survey, with all respondents taking no more than five minutes to provide feedback. Impressively, 95% of users reported that operating the Indigo Home Automation System posed minimal difficulty, while only 5% found it somewhat challenging.

Overall, the user feedback underscores the system's strengths, identifies areas for potential improvement, and provides valuable insights for further enhancing the user experience and system performance.

V. CONCLUSION

In conclusion, this paper has introduced an embedded fingerprint-based attendance management system, seamlessly integrated into a broader framework of fingerprint recognition and authentication relying on minutiae points. The system adeptly captures the local characteristics of fingerprints, specifically the minutiae points within a template, with templates undergoing matching processes during both registration and verification phases.

To enhance quality control, a matching score was strategically incorporated, serving as a decisive factor in evaluating the success of operations. This matching score acts as a threshold, allowing only minutiae data sets surpassing the specified score to be accepted, while those falling below are systematically rejected. The utilization of the minutia score matching method ensures robust fingerprint recognition before attendance records are finalized.

The developed system stands as a significant advancement, notably contributing to time savings for students and lecturers, promoting eco-friendly practices by reducing paper usage, and facilitating timely report generation. Furthermore, the system efficiently records clock-in and clock-out times for individuals, leveraging fingerprint technology to thwart impersonation attempts and curtail absenteeism. Beyond its primary functions, the system plays a pivotal role in alleviating administrative burdens, minimizing human errors, preventing proxy punching, resolving time-related disputes, and facilitating the seamless update and maintenance of attendance records. In essence, the presented fingerprint-based attendance management system emerges as a sophisticated solution that addresses multiple challenges in conventional attendance tracking, ultimately enhancing efficiency and accuracy.

REFERENCES

[1]. Kadry S. and Smaili M (2010): Implementation of a Wireless Attendance Management System Utilizing Iris Recognition Technology. Scientific Research and Essays Vol. 5(12), pp. 1428-1435, 18 June, 2010.
[2]. Khan B., Khan M. K. and Alghathbar K. S.(2010): Implementation of Biometric Solutions for Identity Management in Homeland Security Applications within the Saudi Arabian Context. African Journal of Business Management Vol. 4(15), pp. 3296-3306, 4 November, 2010.
[3]. Bevan S and Hayday S. (1998): Attendance Management: A Review of Good Practice" Report 353, Institute for Employment Studies.
[4]. McKeehan D.A. (2002): Attendance Management Program, The City of Pleasanton, Human Resources.
[5]. Ononiwu G. C and Okorafor G. N (2012): Development of an Attendance System Utilizing Radio Frequency Identification (RFID) Technology Integrated with Automatic Door Mechanism, Published in Academic Research International. Vol 2, No 2, March, 2012.
[6]. Shoewu O., Olaniyi O.M. and Lawson A. (2011): Embedded Computer-Based Lecture Attendance Management System. African Journal ofComputing and ICT. Vol 4, No. 3. P 27- 36, September, 2011.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR2165

[7]. Shehu V. and Dika A. (2011): Integration of Real-Time Computer Vision Algorithms in Automated Attendance Management Systems. Presented at the 32nd International Conference on Information Technology Interfaces (ITI 2010), June 21-24, 2010, Cavtat, Croatia.
[8]. Mehtre, B. M. (1993): Fingerprint image analysis for automatic identification. Machine Vision and Applications 6, 2 (1993), 124- 139.
[9]. Jain A. K., Maio D., Maltoni D., and Prabhakar S. (2003): Handbook of Fingerprint Recognition, Springer, New York, 2003.
[10]. Maltoni D. and Cappelli R. (2008): Fingerprint Recognition, In Handbook of Biometrics, Springer Science + Business Media, U.S.A.
[11]. Ravi. J. K., Raja b. and Venugopal. K. R. (2009): Fingerprint Recognition Using Minutia Score Matching, International Journal of Engineering Science and Technology Vol.1(2), 2009, 35-42. Sharat S. Chikkerur (2005): Online Fingerprint Verification System, A M. Tech Thesis, Affiliation with the Department of Electrical Engineering, Graduate School, State University of New York, Buffalo..
[12]. Md. Saidur Rahman, Fahrin Rahman, Md. Hazrat Ali, Tuhin Ahmed, and Md. Rabiul Islam. "Development and Deployment of an Intelligent Refrigerator System." Published in the Journal of Electronics, Computer Networking, and Applied Mathematics, Volume.3 no. 01, pp. 27–40, Jan. 2023.
[13]. Md. Saidur Rahman, Md. Abdullah Kawser, K. M. Rumman, Fahrin Rahman, and Rubab Ahmmed. "Development and Implementation of an Intelligent Railway System." Published in the Journal of Intelligent Systems for Railway Applications (JIPIRS), Volume 2, Issue 5, pages.