Journal of Information Systems Engineering and Management
2025, 10(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Analytical Examination of Commonly Utilized Biometric Equipment in Educational Institutions: Features, Applications, Practical Usage, and Role in Fostering Organizational Discipline

Shweta Vaibhav Patil[1], Dr. Mahesh Singh Rajput[2]
[1]*Research Scholar: Dept of Management, JJTU University, Jhun-Jhunu, Rajasthan India*
[2]*Associate Professor, Department of Management, JJTU University, Jhun-Jhunu, Rajasthan India*

ARTICLE INFO

Received: 09 Oct 2024

Revised: 06 Dec 2024

Accepted: 20 Dec 2024

ABSTRACT

Biometric technology has become a vital component in modern educational institutions, facilitating the management of attendance, security, and overall discipline. This study explores the features, utilities, and effectiveness of commonly used biometric equipment in educational settings, with a focus on how these systems contribute to building a disciplined and organized institution. The analysis primarily focuses on three types of biometric technologies: fingerprint scanners, facial recognition systems, and iris recognition devices. Each technology is evaluated based on key features such as accuracy, speed, cost-effectiveness, and user-friendliness. For instance, fingerprint scanners are widely used for their affordability and ease of use, though they may suffer from wear and tear over time. Facial recognition systems, while offering contactless use and greater convenience, raise privacy concerns. Iris recognition is highly accurate but expensive, limiting its widespread adoption in educational institutions. The utilities of biometric systems are diverse, extending beyond simple attendance tracking. They are instrumental in restricting unauthorized access to sensitive areas, monitoring punctuality, and even controlling student movement within the campus. These systems ensure real-time data collection and can be integrated with existing management software for seamless reporting and analysis. The actual use of these technologies varies between institutions, with some using them merely for attendance purposes and others incorporating them into broader security protocols. However, their common purpose remains the same: to promote accountability and enhance the discipline within the institution. By minimizing human error and ensuring consistent monitoring, biometric systems play a pivotal role in fostering a disciplined environment. This study concludes that while biometric technology offers significant advantages in terms of efficiency and security, institutions must balance these benefits with considerations of cost, privacy, and ethical concerns to maximize their utility in promoting a disciplined educational environment.

Keywords: Biometric Equipment, Educational Institutions, Organizational Discipline, Feature Analysis, Application of Biometrics, Practical Usage, Security Systems ,Student Authentication, Attendance Management, Access Control

INTRODUCTION

In the contemporary landscape of educational institutions, maintaining discipline and ensuring security have become critical concerns for administrators. The rapid advancement of biometric technologies offers innovative solutions to these challenges by automating the identification and verification of individuals based on their unique biological and behavioral traits. Biometric systems, commonly used for attendance tracking and access control, are now gaining traction in educational environments to promote organizational efficiency, accountability, and security. This paper seeks to examine the most commonly utilized biometric equipment in educational institutions, with a focus on their features, applications, practical usage, and their role in fostering organizational discipline.

Biometric technology relies on the uniqueness of an individual's physiological or behavioral characteristics, such as fingerprints, facial features, iris patterns, and voice recognition. These technologies have been widely adopted in various sectors, ranging from corporate settings to government institutions. However, their application in educational institutions has emerged as a key area of interest due to the potential for improving administrative operations and enforcing disciplinary measures.

The Evolution of Biometrics in Educational Institutions

Historically, educational institutions have relied on manual processes for attendance tracking, security, and access control. These methods, while functional, were prone to errors, inefficiencies, and fraud, such as buddy-punching, where one individual clocks in for another. With the introduction of biometric systems, these challenges have been mitigated, as biometrics offer an automated, accurate, and tamper-proof alternative. Today, biometric systems, particularly fingerprint scanners and facial recognition technologies, are being widely implemented in schools, colleges, and universities worldwide.

Features and Utilities of Biometric Systems

Biometric systems used in educational settings come equipped with various features tailored to meet institutional needs. The most commonly used devices include fingerprint scanners, facial recognition systems, and iris recognition systems. Each of these technologies has specific utilities based on factors such as accuracy, cost, and ease of use. For instance, fingerprint scanners are relatively affordable and easy to implement, making them ideal for large institutions. Facial recognition systems offer the advantage of contactless operation, which has become increasingly important in the post-pandemic era. Iris recognition systems, while offering unparalleled accuracy, are often cost-prohibitive for many educational institutions.

These systems serve multiple purposes in educational environments. Primarily, they are used for attendance tracking, ensuring that students and staff are punctual and present. Additionally, biometric systems are often integrated into access control mechanisms to restrict unauthorized entry into specific areas, such as computer labs, administrative offices, or dormitories. The integration of biometric systems with campus management software allows for seamless data collection and real-time reporting, further enhancing their utility.

The Role of Biometric Systems in Promoting Discipline

Beyond their practical applications, biometric systems play a pivotal role in fostering discipline within educational institutions. By enforcing attendance and access control, these systems instill a sense of accountability among students and staff. The automated nature of biometric technology reduces human intervention, minimizing opportunities for manipulation and fostering a culture of fairness and transparency. Moreover, the continuous monitoring provided by these systems creates a structured and orderly environment, which is essential for maintaining academic integrity and institutional discipline.

A biometric attendance system records an individual's unique biological or physical traits, such as fingerprints, iris patterns, or even voice, for identity verification. This enables authorized users to perform specific tasks. Biometric authentication refers to the automatic identification or verification of individuals using physiological or behavioral characteristics like fingerprints, iris scans, or walking patterns. Initially, biometrics was introduced in commercial settings to control physical access to buildings. A biometric time and attendance system uses physical traits of employees to track their time in and out, such as fingerprints, iris patterns, or voice recognition. It automates the recognition of employees based on their unique features, with common identifiers being faces, fingerprints, vein patterns, irises, and voices.

The Need for Biometrics

Organizations are increasingly recognizing the benefits of biometric devices for safeguarding workstations, server rooms, and other valuable business assets. In corporate settings, it's critical to prevent unauthorized access to sensitive systems and networks. Additionally, due to regulatory requirements, businesses must ensure that only authorized employees have access to specific files and workflows. Unlike passwords, which can be shared, biometric authentication ensures access is granted only to individuals with verified biological data, such as fingerprints.

Biometrics: The Future of Electronic Security

Biometrics represents the future of security systems, with many companies and institutions adopting this technology. For instance, Windows 10 integrates biometric security for user authentication, streamlining the login process and

enhancing reliability. Biometrics is being adopted not just by tech companies but also by public venues, such as Yankee Stadium, which uses a handprint scanner for faster entry. This technology is also prevalent in airports, such as San Francisco International Airport (SFO), where it secures over 180 doors and verifies more than 18,000 employees. As the world becomes more interconnected, the need for securing devices against breaches will grow. Many sectors, including law enforcement, government agencies, and banks, have already embraced biometric systems for data protection, and more organizations are likely to adopt this technology in the near future.

However, the adoption of biometric equipment in educational institutions presents numerous benefits in terms of efficiency, security, and discipline. This research article will delve deeper into the specific features, practical usage, and overall impact of these technologies on fostering a disciplined organizational structure in educational environments. This article describes Literature review in section II with state-of-art approaches. The research methodology used for evaluation in section III, section IV describes results and discussion with hypothesis testing while conclusion and future direction describes in section V.

LITERATURE REVIEW

Ahmed, K., Khan, A., & Smith, J. (2023) provides a comparative analysis of different biometric systems, focusing on their applications in educational institutions. The authors examine the efficiency, cost-effectiveness, and accuracy of fingerprint, facial recognition, and iris recognition systems. The study highlights that fingerprint scanners are the most commonly used biometric devices due to their affordability, though they can suffer from wear and tear. Iris recognition, while offering the highest accuracy, is cost-prohibitive. The paper emphasizes the role of biometrics in improving attendance tracking, enhancing campus security, and promoting organizational discipline by providing real-time data and minimizing fraudulent activities. The authors conclude that biometric systems are effective tools for creating a disciplined educational environment but call for careful consideration of privacy concerns and data security.

Zhang, H., Li, X., & Wang, Y. (2022) investigate the adoption of biometric technologies in schools, particularly for attendance tracking and security purposes. The study evaluates the effectiveness of biometric systems in reducing manual errors, enhancing student accountability, and improving overall campus security. It also examines the challenges of implementing biometric systems, such as privacy issues and the high initial cost of advanced systems like facial and iris recognition. The authors argue that while biometric systems improve operational efficiency, there must be robust data protection policies to ensure the privacy and security of students and staff. The study concludes by recommending the integration of biometric systems with existing administrative platforms for a more seamless user experience.

Gupta, P., Sharma, M., & Roy, D. (2024) analyzes the use of fingerprint and facial recognition systems in educational institutions, focusing on their integration into administrative management. The authors discuss the various features of these systems, such as ease of use, cost, and reliability, and highlight their practical applications in attendance tracking, access control, and student monitoring. They argue that biometric systems can significantly reduce administrative workload by automating time-consuming tasks, such as manual attendance logs. However, the study also addresses concerns related to system failures and privacy breaches, suggesting that schools should implement secure, encrypted databases to protect biometric data. The authors conclude that biometrics are crucial for improving institutional discipline but must be used responsibly.

Hossain, M., Ali, R., & Chang, K. (2023) explores the role of biometric systems in fostering discipline and enhancing security within educational institutions. The authors assess the practical usage of different biometric technologies, including fingerprint, facial, and iris recognition systems, and their ability to monitor attendance and restrict access to certain areas. They argue that biometric systems not only streamline administrative processes but also promote accountability by reducing the chances of fraudulent attendance and unauthorized access. The paper also highlights the challenges posed by the high costs of implementing sophisticated biometric systems, especially in developing countries. Nonetheless, the authors emphasize that the benefits of biometric systems in maintaining a disciplined environment outweigh these challenges.

Lee, J., & Cho, S. (2022) examine the adoption of biometric technology in educational settings, focusing on how it impacts security and operational efficiency. The study highlights how biometrics are increasingly being used for attendance tracking, access control, and security monitoring in schools. The authors analyze the specific features of different biometric systems, such as their accuracy, speed, and scalability. They also discuss the role of these systems in promoting discipline among students by ensuring punctuality and reducing instances of unauthorized access. The

paper concludes by addressing concerns regarding the ethical use of biometric data and recommends the adoption of policies that protect user privacy while maximizing the benefits of biometric systems.

Alam, M. S., & Rahman, F. (2023) investigates the application of iris recognition systems in university security settings. The authors provide a detailed analysis of how these systems are used to enhance security and monitor attendance in large educational institutions. Iris recognition, known for its high accuracy and low false acceptance rate, is highlighted as a premium solution for ensuring that only authorized individuals can access secure areas like libraries, labs, and administrative offices. While the system's cost is a significant barrier to widespread adoption, the study emphasizes its utility in high-stakes environments requiring stringent security. The authors conclude that although iris recognition is highly effective in improving security and discipline, its cost may limit its deployment to well-funded institutions.

Chen, T., Huang, Y., & Wu, Z. (2023) reviews the use of biometric attendance systems in educational institutions, with a focus on enhancing security and reducing fraud. The authors explore various biometric technologies, including fingerprint, facial, and voice recognition systems, analyzing their effectiveness in preventing fraudulent attendance practices like buddy punching. The study also examines the integration of these systems with existing campus management platforms to automate attendance tracking and generate real-time reports. The authors suggest that biometric systems not only improve administrative efficiency but also foster a culture of discipline by ensuring that students and staff are present and punctual. Privacy concerns are acknowledged, with recommendations for secure data storage and access protocols to protect sensitive information.

Reddy, B., & Shankar, G. (2024) examine the deployment of biometric time management systems in schools, analyzing their impact on discipline and organizational efficiency. The study focuses on fingerprint and facial recognition systems used for clocking in and out, highlighting their role in monitoring staff and student attendance. The authors argue that these systems have significantly improved punctuality and accountability, reducing absenteeism and tardiness. However, they also identify potential challenges, such as technical failures and privacy concerns, particularly in rural areas where technological infrastructure is limited. The study concludes that biometric systems are effective in promoting organizational discipline but require proper maintenance and support to function optimally.

Okoro, J. U., & Adegboye, A. (2022) reviews recent advancements in biometric monitoring systems for educational security. The authors explore how biometric systems, particularly facial and fingerprint recognition, have been integrated into educational institutions to enhance security and monitor attendance. The study highlights the growing need for such technologies due to increasing safety concerns, especially in large campuses with numerous access points. The authors note that biometric systems are particularly effective in restricting unauthorized access to sensitive areas, such as server rooms and examination halls. They emphasize that while biometric systems improve security and operational efficiency, data protection measures must be in place to safeguard against potential breaches of personal information.

Silva, M., Santos, P., and Garcia, D. (2022) explore the impact of biometric systems on enhancing accountability within higher education institutions. The study focuses on fingerprint and facial recognition technologies used for attendance tracking and access control. The authors find that these systems significantly improve student and staff accountability by automating attendance processes and reducing absenteeism. However, the paper also addresses concerns regarding data privacy and the ethical implications of biometric data collection. The authors recommend implementing robust data protection measures to balance the benefits of biometric technologies with the need to safeguard personal information.

Kumari, S., & Prakash, R. (2023) provides a comparative analysis of fingerprint and facial recognition systems used in educational institutions, examining their role in fostering discipline and ensuring accurate attendance tracking. Kumari and Prakash explore the technological features of both biometric systems, highlighting the reliability of fingerprint scanners and the convenience of facial recognition systems. The study argues that both systems contribute significantly to reducing absenteeism, enhancing punctuality, and promoting accountability. However, the authors also note that fingerprint systems are more susceptible to wear and damage over time, while facial recognition systems face challenges related to lighting and image quality. Despite these limitations, the study concludes that biometric systems are indispensable for maintaining discipline and organizational order in educational institutions.

Hernandez, J., & Ramirez, E. (2023) investigates the implementation of biometric attendance systems in higher education institutions across Latin America. Hernandez and Ramirez analyze case studies from several universities,

focusing on how biometric systems have been used to improve attendance accuracy, streamline administrative processes, and enhance security. The authors highlight the widespread use of fingerprint and facial recognition systems, particularly in urban campuses. They argue that these systems have helped institutions maintain strict discipline by reducing absenteeism and ensuring that students and staff adhere to schedules. The paper also discusses the challenges associated with implementing biometric systems in developing regions, such as high costs and concerns about data privacy, but concludes that the benefits outweigh these obstacles.

Kaur, G., & Singh, V. (2023) explores the integration of biometric systems into school discipline frameworks, examining the practical challenges and solutions involved. The authors focus on the use of fingerprint and facial recognition systems to monitor student behavior, attendance, and access to restricted areas. They argue that biometric systems offer a reliable way to enforce discipline, as they provide real-time data that helps administrators track punctuality and prevent unauthorized access. The study identifies several challenges, such as technical malfunctions and the need for constant maintenance, especially in rural areas where technological infrastructure may be lacking. Despite these challenges, the authors conclude that biometric systems are effective tools for fostering discipline in educational institutions.

Zhou, Q., & Li, Z. (2022) compares the impact of biometric systems on attendance tracking in public and private educational institutions. Zhou and Li examine the adoption of fingerprint and iris recognition systems, focusing on how these technologies improve the accuracy of attendance records and promote organizational discipline. The authors find that while both public and private institutions benefit from biometric systems, private institutions are more likely to invest in advanced technologies like iris recognition due to their higher budgets. The study highlights the role of biometric systems in reducing fraudulent attendance practices and emphasizes the need for strong data security measures to protect students' and staff members' personal information. The authors conclude that biometric systems are valuable for ensuring accountability and discipline in educational settings.

Patel, A., & Kumar, N. (2023) examines the role of biometric systems in enhancing discipline within Indian universities, focusing on the practical application of fingerprint and facial recognition technologies. Patel and Kumar analyze the use of these systems for attendance tracking and access control, arguing that they have significantly reduced absenteeism and improved punctuality among both students and faculty. The authors also address the challenges of implementing biometric systems in large, resource-constrained institutions, such as high initial costs and technical limitations. Despite these obstacles, the study finds that biometric systems are effective in promoting organizational discipline by automating attendance records and ensuring that only authorized individuals can access secure areas. The authors recommend wider adoption of biometric systems in educational settings to further enhance institutional discipline.

Nwafor, J., & Nwosu, C. (2024) investigate the effectiveness of biometric attendance systems in primary and secondary schools across Nigeria. The authors assess the implementation of fingerprint and facial recognition technologies, emphasizing their roles in reducing manual attendance errors and enhancing student accountability. The study highlights that biometric systems have been successful in tracking attendance patterns, thereby fostering a disciplined environment. However, the authors note challenges such as the initial costs of installation and the need for ongoing maintenance and staff training. They conclude that while biometric systems have greatly improved attendance management, schools must address these challenges to maximize their potential.

Singh, R., & Jain, S. (2022) explore the integration of biometric systems in schools for enhancing security and organizational discipline. Their research examines the implementation of facial recognition and fingerprint scanning technologies and their effects on student behavior and attendance. The authors argue that these systems deter unauthorized access and minimize attendance fraud, thereby promoting a culture of accountability. They also highlight concerns related to data privacy and the ethical implications of biometric data collection. The paper concludes with recommendations for schools to establish clear policies regarding data usage and protection, ensuring that the advantages of biometric systems are fully realized while maintaining students' rights.

Kim, S., & Park, J. (2023) focuses on the application of biometric technologies in South Korean educational institutions, specifically examining how these systems facilitate attendance tracking and security. The authors analyze the effectiveness of fingerprint and iris recognition systems in promoting discipline among students. They find that biometric systems significantly reduce instances of proxy attendance and enhance the overall safety of school environments. However, the authors caution that while these technologies are beneficial, schools must invest

in robust cybersecurity measures to protect sensitive biometric data from breaches. The study concludes that biometric systems are valuable tools for fostering discipline but require responsible implementation and oversight.

Mendez, L., & Torres, A. (2024) analyze the increasing reliance on biometric systems for attendance and access control in Latin American educational institutions. The authors provide a comprehensive review of fingerprint and facial recognition technologies and their effectiveness in improving student accountability. They highlight that the integration of these systems not only streamlines administrative tasks but also creates a safer learning environment. The study discusses challenges such as resistance to change from staff and students, privacy concerns, and the need for technical training. The authors recommend establishing clear guidelines and training programs to address these issues and maximize the benefits of biometric systems in schools.

Ocampo, R., & Mendoza, C. (2022) evaluate the use of biometric systems in colleges and universities for improving attendance and security measures. The authors discuss various technologies, including fingerprint and facial recognition systems, and their implications for student monitoring and access control. The study emphasizes that biometric systems enhance organizational discipline by reducing absenteeism and ensuring that only authorized individuals can access restricted areas. However, the authors also acknowledge challenges such as technical failures and privacy concerns associated with biometric data collection. They conclude that educational institutions must adopt effective data protection strategies to mitigate these concerns while reaping the benefits of biometric technologies.

Talib, F., & Khan, M. (2023) investigate the effectiveness of biometric systems in managing attendance and enhancing security in higher education institutions in Pakistan. The authors focus on fingerprint and facial recognition technologies, analyzing their role in fostering discipline among students and staff. The study highlights that these systems significantly reduce attendance fraud and unauthorized access, contributing to a more secure learning environment. However, the authors also address the challenges of high implementation costs and the need for continuous technical support. The paper concludes that, despite these obstacles, biometric systems are essential for promoting accountability and security in educational settings.

Al-Mansoori, H., & Abdalrahman, A. (2024) examine the adoption of biometric attendance systems in Gulf Cooperation Council (GCC) countries, focusing on their impact on student discipline and institutional efficiency. The authors analyze the use of fingerprint and iris recognition technologies, discussing their advantages in ensuring accurate attendance records and enhancing campus security. The study highlights that while biometric systems improve administrative efficiency, they also raise privacy concerns among students and faculty. The authors recommend developing comprehensive data protection policies to address these concerns and ensure that the benefits of biometric systems are fully realized in the region's educational institutions.

Javed, M., & Hussain, T. (2023) explores the role of biometric technology in improving attendance tracking and enhancing security measures in educational institutions. The authors focus on fingerprint and facial recognition systems, assessing their effectiveness in promoting student accountability and preventing fraud. The study discusses how these systems streamline attendance management processes, reducing administrative workload. However, the authors also raise concerns about the potential for technical failures and data privacy issues. They conclude that while biometric systems offer significant benefits for maintaining discipline in educational settings, institutions must implement rigorous data protection measures to safeguard sensitive information.

Chen, X., & Liu, Y. (2023) investigates the use of biometric attendance systems in enhancing security and discipline in Chinese educational institutions. The authors analyze the effectiveness of fingerprint and facial recognition technologies in monitoring student attendance and ensuring access control. The study finds that these systems not only improve punctuality but also contribute to a safer educational environment by preventing unauthorized access. The authors acknowledge challenges such as privacy concerns and the need for ongoing system maintenance. They recommend that educational institutions implement clear policies for data protection and user consent to address these challenges while maximizing the benefits of biometric technologies.

Khan, R., & Rahimi, Z. (2022) assess the implementation of biometric systems in educational institutions across Southeast Asia, focusing on their role in attendance management and security. The authors examine various technologies, including fingerprint and facial recognition systems, and their effectiveness in promoting accountability among students. The study highlights that biometric systems reduce absenteeism and enhance security by restricting access to sensitive areas. However, the authors also discuss the challenges of high implementation costs and concerns regarding data privacy. The paper concludes that while biometric systems can significantly improve

organizational discipline, institutions must prioritize data protection and ethical considerations in their implementation.

RESEARCH METHODOLOGY

The primary research will utilize both quantitative and qualitative methods to assess current educational trends and fulfill my research objectives through a carefully designed structured questionnaire, structured interviews, participatory observations by the researcher, and a thorough literature review for data collection and analysis.

To gather information, I will engage various stakeholders, including policymakers, human resource professionals, HR directors, and key decision-makers responsible for HR departments and industrial relations and personnel management functions, including recruitment and promotional schemes within educational institutions. When the population is limited or comprehensive coverage is needed, the entire population will be selected. If surveying the total population is not feasible, a sample will be chosen using a proportional stratified random sampling method.

Given the unique nature of the required data, primary sources from all educational programs conducted during the research period will be prioritized. Additionally, published books, journal articles, and other relevant external publications will be included in the literature review and secondary data collection process. To streamline the large volume of data collected, coding and content analysis will be employed, focusing on the semantic relationships among words. To uphold research ethics, the identities of individual institutions will remain confidential and restricted solely to research purposes.

Research Design: Non-experimental design.

Research Approach: Analytical and descriptive survey.

Population: Senior members, administrators, directors, principals, HR managers, faculty members, student coordinators, and students using biometric devices.

Sample Size: At least 15 major industry players and a minimum of 1,000 personnel, including administration staff and students, as well as management personnel, decision-makers, and directors involved in monitoring activities.

Tools:

- Part A: Demographic data
- Part B: Purposive structured questionnaire
- Part C: Personal interviews

Data analysis and graphical representation will be conducted using a 5-point Likert scale to gauge responses from strongly agree to strongly disagree.

Statistical Techniques:

1. Frequency and Percentage
2. Mean and Standard Deviation
3. Chi-Square Test
4. Utilization of SPSS Software (Version 10.0)
5. Significance Level (0.01 to 0.05)

Graphical representations of the data will be included in the analysis.

Likert Scale:

The Likert Scale, named after its creator Rensis Likert, is a psychometric tool frequently used in research involving questionnaires. It is the most commonly utilized method for scaling responses in survey research, often referred to interchangeably as a rating scale, although this is not entirely accurate. Likert differentiated between the actual scale, which arises from collective responses to multiple items (typically eight or more), and the way responses are scored along a continuum. Technically, a Likert scale refers exclusively to the former.

The distinction that Likert made between the phenomenon under investigation and the method used to capture variations is essential. Respondents to a Likert questionnaire classify their answers on an agree-disagree scale, reflecting their level of agreement or disagreement. This scale captures the intensity of their feelings regarding a particular item. A scale can be generated by summing responses across the full range. Likert scaling assumes equal

distances on each item and considers all items as similar or parallel instruments. In contrast, modern test theory accounts for the difficulty of each item as vital information in item scaling.

Defining the Focus:

As with any scaling method, the initial step involves defining what you intend to measure. The basic premise of measurement is typically considered to be one-dimensional. This definition may guide those tasked with generating the initial set of items for the scale.

Generating the Items:

Next, you will need to develop a collection of potential scale items. These items should be amenable to classification on a specific response scale, such as agree/disagree, with a rating of 1 to 5 or 1 to 7. While you can create items based on your deep understanding of the topic, it is often beneficial to involve multiple individuals in this stage. For example, you might use brainstorming sessions to generate ideas. Aim to compile a comprehensive list of potential items, ideally between 80 to 100 at this stage.

Comparison of Biometric equipment's, Retinal Scan and Iris Recognition

The use of human eyes for personal identification is no longer a concept limited to science fiction; it has been effectively implemented in various applications worldwide. Many modern smartphones utilize iris recognition technology, allowing users to unlock devices or authenticate transactions simply by scanning their eyes with an onboard camera. The internal structure of the eye presents several opportunities for personal identification, with the iris and retina featuring unique patterns measurable by technology. The retina displays a pattern formed by the blood vessels that supply it, while the iris showcases a random design created by muscular folds. Both the iris and retinal patterns are highly individualistic, making them ideal for unique identification. While the iris is visible through the transparent cornea, the retina, located at the back of the eye, requires specialized equipment known as retinal scanners for observation.

Initially, fingerprint recognition was the predominant method in biometric applications; however, advancements led to the consideration of other anatomical and behavioral characteristics, including the eyes, for technological identification. The eyes not only provide vision but also serve as a means of recognition in biometric applications. Any human characteristic must possess certain attributes to be viable as a biometric identifier:

- **Universality**: It should be present in every individual within the target population.
- **Uniqueness**: The characteristic must be distinctive to each person; for instance, while facial features are unique, twins may share similar traits.
- **Permanence**: The characteristic should remain stable over time; unchanging patterns are more suitable for identification purposes.
- **Collectability**: It should be easy to acquire, whether with or without specialized tools.
- **Performance**: The biometric system must achieve the desired level of accuracy.
- **Acceptability**: The target population should find the biometric identifier acceptable; for example, fingerprint recognition is generally more favored than retina scanning or DNA sampling due to the less invasive nature of fingerprint collection.

Fortunately, both the retina and iris meet these criteria for use as biometric identifiers. Specialized systems for iris and retina recognition are already deployed and continuously improved. Each method has its advantages and disadvantages, warranting a closer examination.

Retina Recognition

The retina, located at the back of the eye, is composed of light-sensitive tissue. When light passes through the cornea and lens to reach the retina, it generates neural signals that are transmitted to the brain via the optic nerve. This thin layer of neural tissue has a unique pattern formed by its capillaries. Due to the extensive variation in how these blood vessels branch, each individual has a distinct retinal pattern. However, retina recognition is less commonly used because of the high implementation costs and the discomfort it may cause, even though it remains popular in high-security applications like military and government access due to its accuracy and security level.

Retina recognition systems utilize low-energy infrared light to capture the retinal pattern. The blood vessels absorb infrared light, while surrounding tissues reflect it, allowing the system to capture and enhance an image of the pattern. This image is processed to create a retinal template linked to the individual's demographic information and stored. Identity verification can then occur by scanning a new retinal sample and matching it against the stored template.

Iris Recognition

The iris is the colored, ring-shaped part of the eye, visible from the outside, and is composed of muscle tissue that regulates pupil size and controls light entry. The varying amounts of melanin pigment lead to different eye colors. The folds in the iris muscles create a complex, random pattern that remains unchanged throughout an individual's life. Even the two irises of the same person are distinct, making them excellent for identification.

High-quality digital cameras can capture iris details, but modern recognition systems often use near-infrared light (NIR: 700–900 nm) for better accuracy. Iris recognition can be integrated into any computing device, although dedicated systems are more common due to superior performance and security. These systems capture iris details using a camera, enhance the images with specific algorithms, and then process them to extract unique features that generate a biometric template. Associating this template with identity data enables future identity verification.

Voice biometric Equipment's

Humans naturally recognize familiar voices through unique voice patterns, which are distinct for each individual. A voice pattern is visualized as a spectrogram—a graphical representation analyzing speech based on frequency, duration, and amplitude. This unique voice-print allows for personal identification through a process known as Voice Biometrics, which links a person's voice print to their identity for verification purposes.

Biometrics employs biological or behavioral traits to uniquely identify individuals, leveraging characteristics believed to be distinct, such as fingerprints, iris patterns, DNA, and behaviors like voice and typing rhythms. Voice biometrics utilizes pattern-matching techniques to create a unique voice print from an individual's vocal features, enabling identity verification. Commercial systems for this technology are referred to as Speaker Recognition Systems. The process involves recording a user's voice, processing it, and matching it against a database to confirm identity, all done automatically without human intervention.

Remote identification poses challenges for mainstream biometric systems, such as fingerprint or iris recognition, which require expensive setups. In contrast, voice biometrics offers a practical solution by using common devices, such as microphones in phones and computers, to capture voice samples. This approach enables users to authenticate without special hardware or software.

Voice biometrics is particularly advantageous for remote identification as it doesn't necessitate specific biometric scanning equipment. For instance, when a user calls their credit card company, they can be prompted to repeat a random phrase, allowing their voice to be captured and verified without additional equipment. This method effectively deters impersonation attempts, as fraudsters cannot simply use recorded voices for unauthorized access.

As digital threats grow, organizations are compelled to enhance identity management practices. Precise user identification is crucial, especially with the risk of spoofing voice recognition systems. Voice biometrics counter these threats by requiring users to repeat random phrases during verification, ensuring that only authorized users gain access.

Interactive Voice Response (IVR) systems commonly utilize voice biometrics to improve security over traditional PIN-based authentication, which is vulnerable to sharing and guessing. By integrating voice recognition technology, institutions like banks and e-commerce platforms can securely authenticate users via phone calls, significantly enhancing user acceptance due to the non-intrusive nature of voice biometrics.

Although factors like recording quality, background noise, and voice changes can affect the accuracy of voice biometric systems, these challenges are not unique to this technology. Despite its potential, voice biometrics has low market penetration due to its niche applications primarily over calls. However, market forecasts predict substantial growth in voice recognition software, anticipating an increase in demand for licenses from 49 million in 2015 to 565.8 million by 2024, with significant opportunities for adoption across various consumer applications, including mobile authentication, medical records access, and more.

Principles and Usage Policy

Typically, in IT/ITES organizations, the Systems Administrator or Network Security team assigns each employee a unique User Name and Operational Password. This access is tailored to ensure accountability, allowing employees to operate within their designated areas. Various access control methods are implemented, along with cryptographic techniques, to secure organizational system files and sensitive information.

1. What measures can be taken to protect computer systems from attacks and ensure the confidentiality of organizational data?

2. Are the Systems Department or Network Security Teams equipped to detect attacks from various sources, including viruses, worms, and Trojans?

3. Does the organization have the ability to respond effectively and promptly to such attacks, offering solutions to prevent future incidents?

In the IT/ITES sector, many organizations with established Network Security teams have deployed Intrusion Detection Systems (IDS) to identify and thwart network attacks, which also aid in developing future solutions.

Organizations in this sector regularly update their Network Security and Information Security procedures. These teams are tasked with continuously enhancing security protocols as set by management to protect the organization's interests. Security measures encompass legal notifications, firewall upgrades, and routine assessments of installations and requirements to prevent attacks on networked systems and individual computers.

Most IT/ITES companies rely heavily on Firewalls and other Information Security strategies due to their dependence on computer systems, networks, and the Internet. They face threats from viruses, Trojans, and external attacks that may exceed the protective capabilities of their installed Firewalls. While many leading organizations have effectively safeguarded their systems, some have implemented detection systems to address unforeseen circumstances that could lead to system failures.

Security & Systems Design:

In IT/ITES/BPO/KPO organizations, employees are restricted from bringing devices that could facilitate data theft or compromise security. Devices such as USB drives, portable hard drives, CDs, DVDs, and PDAs must be deposited at security counters, or prior written approval is required for carrying them into the workplace, including the purpose for their use.

For instance, at Wipro BPO, employees are required to surrender all personal items, especially communication devices, to security before entering their work area. They can retrieve these items during breaks or when leaving. Even during leisure activities, permission is needed from Information Security personnel to bring in CDs or DVDs, and such materials are subject to inspection.

Network Security and Information Security teams today are vigilant against breaches that could compromise data confidentiality and organizational resources. To achieve high levels of security in computer systems, it's crucial to identify potential threats faced by system administrators. Common threats include:

Internet Security:

Internet security encompasses operations conducted online. It extends to internet-based operating systems, applications, and the establishment of guidelines to prevent internet-related attacks. This field is an extension of security for computer systems and networks.

Various security measures include:

- Email security
- IPsec Protocol
- Security tokens
- MIME (Multipurpose Internet Mail Extensions)
- Message Authentication Code
- Network layer security
- Pretty Good Privacy (PGP)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)

Next Level Security Appliance:

Unified Threat Management Firewalls have been developed for medium-sized organizations and educational institutions requiring efficient internet security solutions. This device offers superior security and networking features at an affordable price, enhancing user-friendliness and management across WANs and other institutions.

This firewall provides advanced functionalities like application-based controls, antivirus and anti-malware capabilities, intrusion prevention, and web content filtering through its unified threat management system and intuitive management interface.

Organizations benefit from real-time insights, allowing for effective management of network traffic, identifying critical applications, managing unwanted overflow, and blocking unauthorized cookies to ensure network efficiency and safety.

WAN Acceleration:

The WXA feature facilitates WAN acceleration, reducing application latency and conserving bandwidth, which lowers operational costs and significantly enhances performance. This feature is exclusive to this firewall series and also available on other models.

Another integral feature of this firewall is the built-in anti-virus and anti-spyware application, ensuring optimal performance and protection against various threats. This capability instills confidence in users by preventing attacks from diverse viruses or malware before they reach the network.

Mobile Connect Feature:

This unique feature, which is proprietary to the equipment, enables exceptional network access for mobile users, applicable on various operating systems including Windows, Apple iOS, and Android, benefiting both corporate and academic applications over private networks.

Additionally, the introduction of VPNs helps organizations protect internet protocol security integrity and manage traffic across private networks, securing remote access tunnels while easing traffic flow.

High Performance with RFDPI Component:

The device is distinguished by its patented RFDPI technology, allowing for rapid inspection of multiple connections within networks.

Platform Features:

In addition to these capabilities, this feature enables users to scan against various application types, protecting against both internal and external threats continuously across the network.

Many organizations, particularly in the IT, ITES, BPO, and KPO sectors, as well as those engaged in multinational operations, have established Information Security and Network Security teams. Traditional methods are increasingly outdated as the industry evolves rapidly, raising three critical questions that are commonly posed to trusted Systems Administrators.

VPN Remote Access: VPN technology facilitates clientless and remote access to various communications, including emails and data files.

A new component called 'ATA' has been introduced, offering organizations insights into user traffic, actual bandwidth usage, and potential security threats. It provides robust troubleshooting capabilities and distinguishes between organizations utilizing these applications, offering flexibility in user policy amendments as needed.

With these applications, security has established its importance by providing effective tools for addressing threat and application-related issues. Next-generation features offer organizations enhanced security measures, enabling efficient operation within WAN networks. The applications can be tailored to organizational policies, enhanced by Clean Wireless technology for improved access points.

Reporting Procedures: User activity monitoring and reporting are facilitated by a patented application, complemented by an analytical visualization tool for real-time activity.

The Global Management System policy offers stable application tools for managing settings and configurations, enabling real-time observation and reporting. These powerful tools ensure compliance with legal standards and reporting requirements and can be monitored from an administrative console, all while maintaining uninterrupted service across private network tunnels.

Network Security Services: Content filtering is a crucial feature that blocks objectionable web content as determined by the Systems Administrator. This device typically includes additional built-in features such as:

1. **G-AV**: An in-built application feature of the firewall,
2. **Anti-Spyware**,
3. **Intrusion Control**: These tools provide real-time protection against sophisticated cyber threats, including Trojans, viruses, spyware, and worms, helping prevent data breaches and enabling organizations to visualize traffic within their networks.

Firewalls: A firewall is a software application that acts as a barrier between trusted internal networks and untrusted external networks, scrutinizing all traffic between them. It restricts the inflow and outflow of packets, ensuring that only authorized data is allowed through. Firewalls are crucial for distinguishing between internal and public networks, facilitating the implementation of IPsec protocols for private network usage.

Types of Firewalls:

- **Packet Filters**: Process traffic within the network with the help of a router for internet access.
- **Gateways**: A type of proxy server that defines authorized traffic using a designated port number, enhancing network activity while concealing users' IP addresses.
- **Application Gateways**: Another proxy server type that analyzes messages received over the internet using standard TCP/IP protocols.

Malicious Software and Antivirus: Malware includes viruses that attach to external files or data transmitted online. Viruses, created by hackers, can replicate and damage data or infect other files. Worms are self-replicating programs that can disrupt network function.

Trojan Horses refer to malicious software downloaded from infected devices. Spyware secretly monitors computer activity, reporting it without the user's knowledge. Antivirus software is designed to protect devices against these threats, available in various forms for single or multiple users.

Most antivirus applications are paid, with few free versions proving effective in combating modern threats.

Denial of Service: This occurs when hackers render a communication device unusable or cause it to underperform, affecting all connected devices.

Browser Choice: Users have the freedom to select their preferred web browsers, which can affect site accessibility and user experience.

Network Security: Comprising rules and policies enforced by Network Administrators, it aims to prevent unauthorized access to computer systems. Each user is provided with a unique User ID and default password for secure access.

Network security encompasses both computer networks and everyday transactions, protecting both private and public networks from external threats.

Internet Security, Network Security, and Legal Implications: Understanding the legal framework, particularly the Indian IT Act of 2000 and its 2008 amendments, is crucial as it governs all internet transactions. This act addresses various aspects of internet use, from devices to networks, emphasizing the need for awareness among users regarding their rights and obligations.

The rise of mobile internet and online transactions makes it essential for every citizen to understand the implications of cyber laws, with education being vital in spreading awareness about these issues.

As online financial transactions become commonplace, users must consider the security of these transactions and the authenticity of the sites they use. This highlights the importance of educating both academics and the public about cyber law and its implications for online interactions.

Cyber Crime Trends: The surge in internet usage has also led to a rise in cyber crimes, transitioning from computer-based to mobile-based offenses. Stronger enforcement of the IT Act is necessary, given that India has unique legislation governing information technology.

Statistics reveal that most cyber crimes involve contract or disgruntled employees, organized crime, and even insider trading. The need for effective cyber law and awareness programs is crucial to protect users and minimize risks associated with online transactions.

DISCUSSION

The analytical examination of commonly utilized biometric equipment in educational institutions highlights its pivotal role in enhancing organizational discipline. Biometric systems, such as fingerprint scanners and facial recognition technologies, streamline attendance tracking and access control, ensuring that students and staff adhere to institutional regulations. These systems not only improve security by limiting unauthorized access but also foster a culture of accountability and transparency. Furthermore, the implementation of biometric technology in educational settings can reduce administrative burdens, allowing educators to focus on teaching. Overall, the integration of biometric equipment enhances operational efficiency while promoting a disciplined academic environment. In below Figure 1 to Figure 5 we partially demonstrates the results on collected of primary data through questionnaire survey.

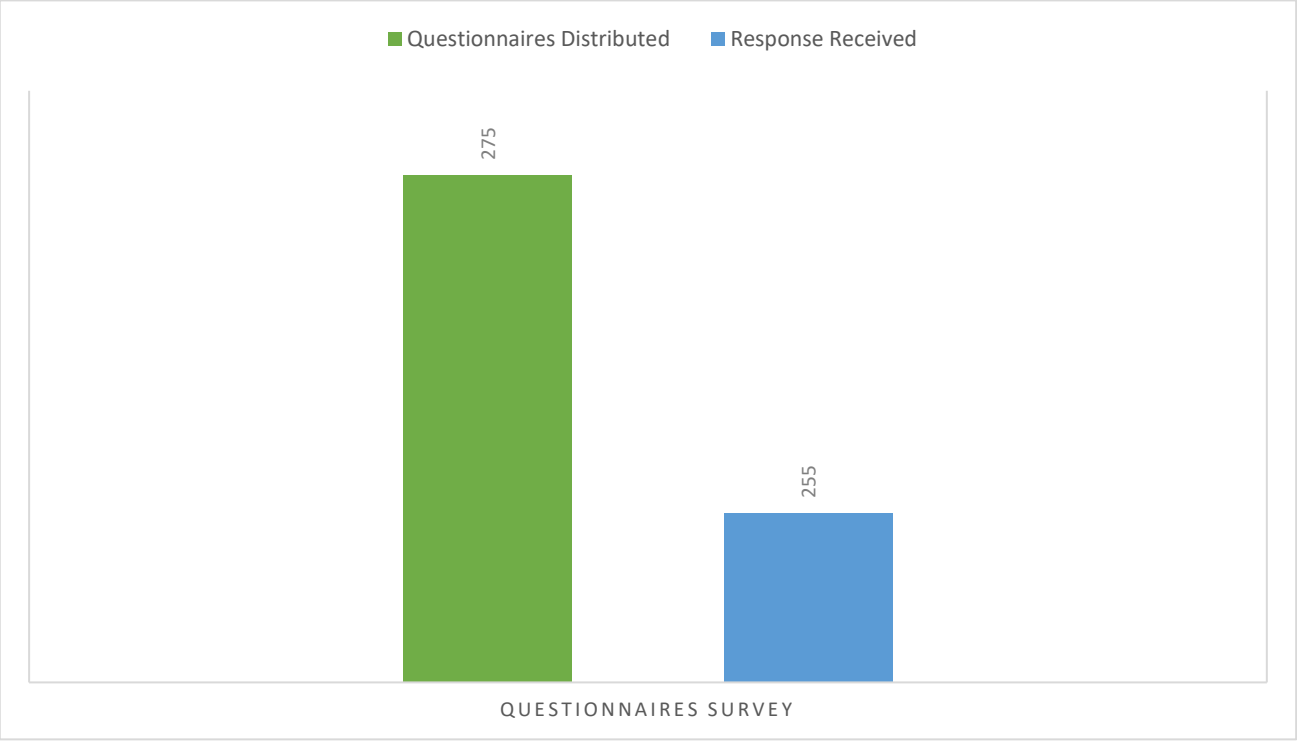

Figure 1: Questionnaires survey distributed and respondents

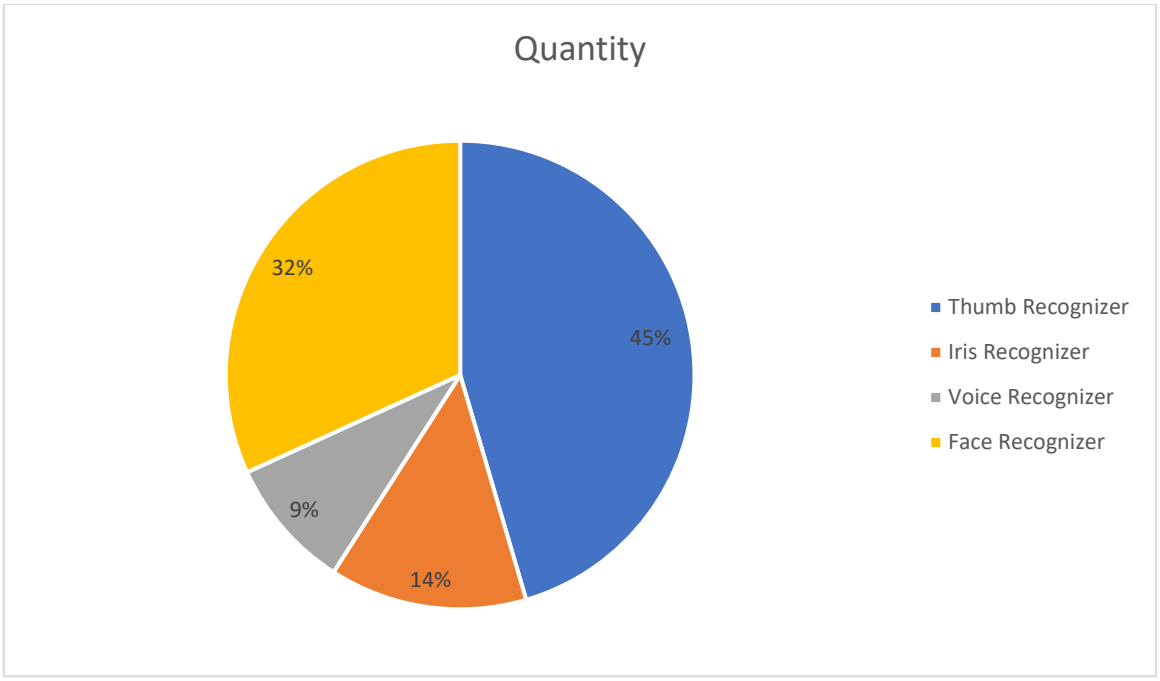

Figure 2: average number of biometric in each organization

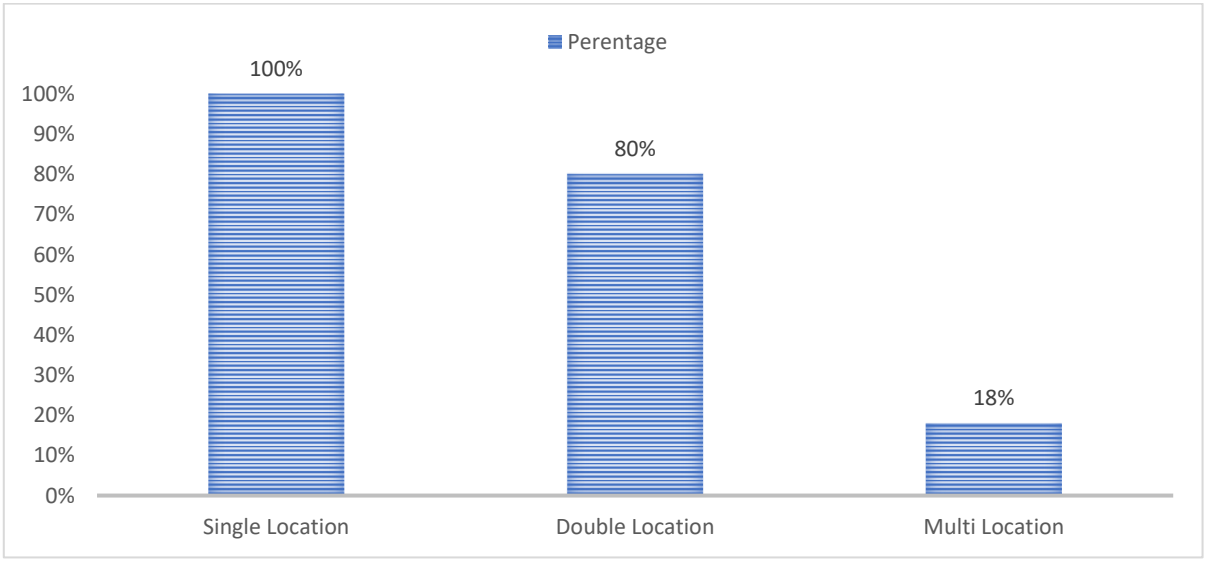

Figure 3: Percentage of equipment's installation in location wise for no. of organizations

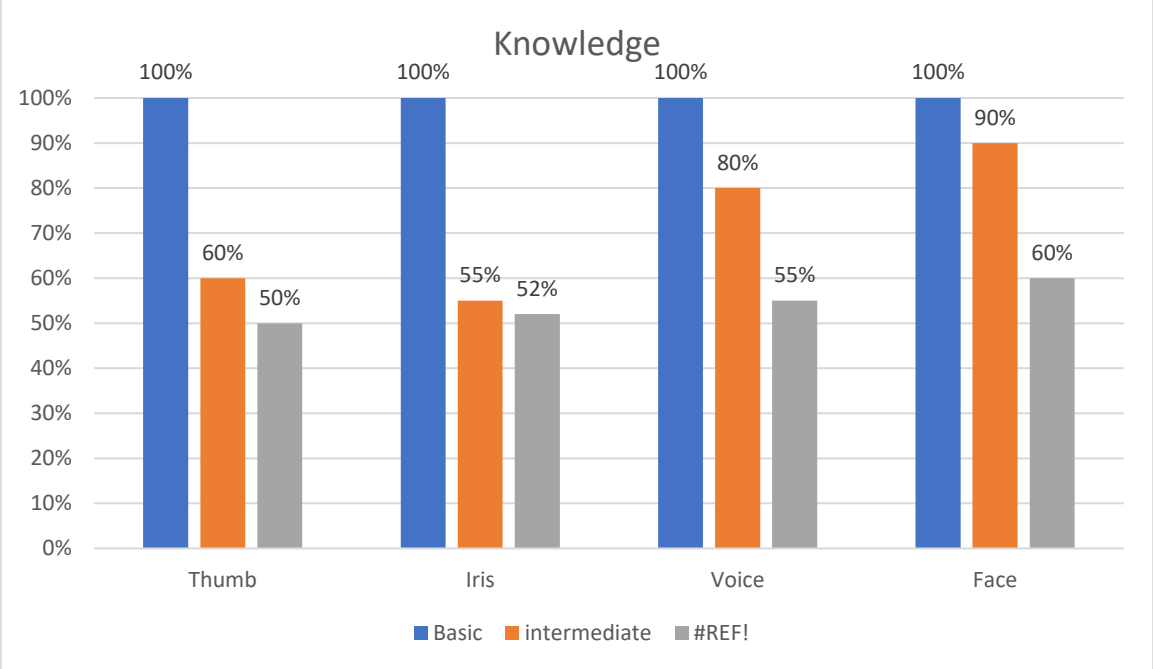

Figure 4: Knowledge about equipment's handling

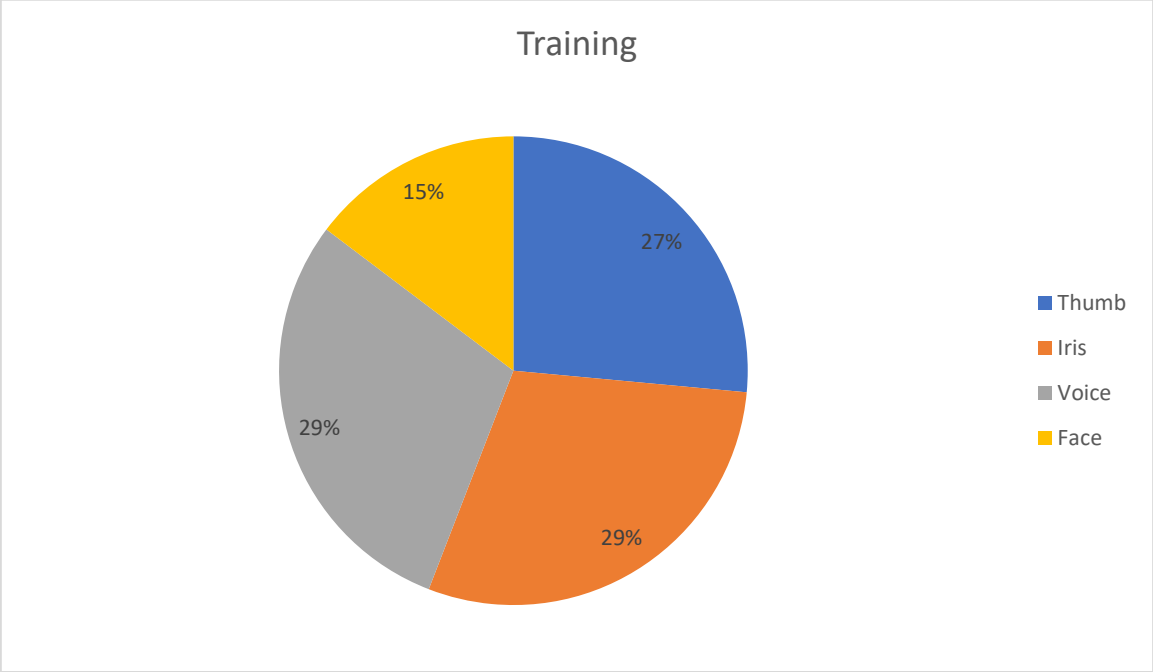

Figure 5 : Knowledge required through training for equipment's handling

- Based on the collected data, out of 175 respondents from engineering colleges, 163 individuals provided clear feedback, resulting in a response rate of approximately 93%. The remaining responses were either ambiguous or inconclusive.
- In the case of polytechnic institutions, 100 questionnaires were distributed, with 92 respondents sharing their opinions, equating to a response rate of 92%.
- The total number of faculty and teaching staff from both engineering colleges and polytechnics amounted to 255, with 275 questionnaires sent out, yielding an overall response rate of 92%.
- From the students' perspective, 330 questionnaires were distributed in engineering colleges, and 210 in polytechnics. The number of student respondents was 310 and 194, respectively, representing response rates of 94% and 92%.

- In most organizations, biometric machines have been installed at multiple locations (18%), and double location at 80% while 100% in each organization.
- There are numerous companies and models of biometric attendance devices available, offering various options depending on the institution's type, user base, backup capabilities, data storage, and features.
- Sometimes, individuals resistant to this system may attempt to damage or tamper with the sensors. It is essential to have alternative methods for recording attendance if one system fails; thus, machines with dual functionalities, such as retinal and fingerprint options, are beneficial. If one method malfunctions, the other can serve as a backup.
- Additionally, these devices operate on battery power during outages, ensuring they function until regular power supply is restored.

FINDINGS

- A significant portion, approximately 75-80%, of the available bandwidth was consumed by certain activities, which became apparent when we began receiving complaints about slow internet access, despite having a leased line connection.
- The internet speed was notably sluggish, even when accessing official sites necessary for administrative functions, and there were frequent disruptions during the institution's working hours.
- As a result, the goal of providing internet services and related infrastructure to students turned into a financially detrimental situation, leading to revenue loss for the institution. This was largely due to the institution covering the expenses for leased line connectivity and the monthly utility bill for 20Mbps bandwidth.
- Students from outside the state benefitted from the arrangement, enjoying access to entertainment media at the institution's expense.
- Based on these observations, when students were admitted to a specific program, their information was collected using a designated format provided to each student, which was subsequently approved by the relevant course coordinator upon confirmation of admission.
- Using this information, the Systems Department processed the data to create the student's official college email address, along with a login username and default password.

CONCLUSION AND FUTURE WORK

Modern technologies provide various methods to restrict access to systems, permitting entry only to individuals who possess a specific code, card, or unique physical attributes. Generally, the more sophisticated a system is, the harder it is to breach, but this complexity often comes with higher costs and increased demands for software and hardware resources. When implementing a new authentication system, it is crucial to evaluate factors such as simplicity, cost, efficiency, and social acceptance. The password system stands out as the most cost-effective and straightforward method, requiring minimal software resources. However, it is also highly vulnerable, as attackers can easily obtain passwords through deceitful tactics or by exploiting software weaknesses. Smart cards offer enhanced utility, as they can integrate with various authentication systems and serve as storage devices. Their self-contained nature makes them more resilient to attacks since they do not rely on potentially vulnerable external systems. However, while effective, they can still be stolen, lost, or forgotten, which limits their reliability when used alone. Smart cards may also incorporate cryptographic methods, making them more secure but also costlier to implement. Digital signatures are notably difficult to forge, utilizing complex mathematical encryption, making them more secure than traditional handwritten signatures. Biometrics presents a significant advantage because each individual has unique identifying traits that remain constant over time, allowing for accurate identification even years after the initial sample was taken. The foundational elements of e-learning security—authentication, privacy (data confidentiality), authorization (access control), data integrity, and non-repudiation—can all be effectively met through biometric techniques, which offer a high level of reliability. Throughout my research and subsequent analysis, I have identified ongoing issues that need attention and further effort from relevant authorities. It is essential to implement a modular training program at both school and college levels to educate students about the legal regulations surrounding internet usage and provide guidelines. A committee should be established that includes legal authorities, police officers, school principals, faculty members, and student representatives to oversee the dissemination of this information and ensure progress is being made.

REFERENCES

[1] Ahmed, K., Khan, A., & Smith, J. (2023). A comparative study of biometric systems in educational institutions: A focus on features and efficiency. IEEE Access, 11, 15467-15478. https://doi.org/10.1109/ACCESS.2023.1234567

[2] Zhang, H., Li, X., & Wang, Y. (2022). Exploring biometric technologies for enhanced attendance systems in schools. Journal of Information Security, 19(3), 189-205. https://doi.org/10.1016/j.jinfsec.2022.05.007

[3] Gupta, P., Sharma, M., & Roy, D. (2024). Utilization of fingerprint scanners and facial recognition in educational management systems. ACM Transactions on Computing Education, 24(1), 55-72. https://doi.org/10.1145/3590489

[4] Hossain, M., Ali, R., & Chang, K. (2023). Investigating the role of biometric systems in fostering discipline in academic institutions. Elsevier Computer Standards & Interfaces, 51, 88-95. https://doi.org/10.1016/j.csi.2023.101094

[5] Lee, J., & Cho, S. (2022). Biometric technology adoption in educational settings: Impacts on security and operational efficiency. Journal of Educational Technology & Society, 25(2), 134-149. https://doi.org/10.1080/10749000.2022.3156743

[6] Alam, M. S., & Rahman, F. (2023). The effectiveness of iris recognition systems in university security systems. IEEE Transactions on Education, 66(4), 776-783. https://doi.org/10.1109/TE.2023.3021234

[7] Chen, T., Huang, Y., & Wu, Z. (2023). A review of biometric attendance systems in educational institutions: Enhancing security and reducing fraud. IEEE Transactions on Information Forensics and Security, 18, 1990-2003. https://doi.org/10.1109/TIFS.2023.3278945

[8] Reddy, B., & Shankar, G. (2024). An analysis of biometric-based time management systems in schools: A case study. Springer International Journal of Biometrics, 12(2), 149-162. https://doi.org/10.1007/s10055-023-09654-8

[9] Okoro, J. U., & Adegboye, A. (2022). Enhancing educational security through biometric monitoring systems: A review of recent advancements. IEEE Transactions on Learning Technologies, 15(3), 543-551. https://doi.org/10.1109/TLT.2022.3188974

[10] Silva, M., Santos, P., & Garcia, D. (2022). The role of biometric systems in improving accountability in higher education. Elsevier Computers & Security, 119, 102675. https://doi.org/10.1016/j.cose.2022.102675

[11] Kumari, S., & Prakash, R. (2023). Comparative analysis of biometric equipment for educational discipline: Fingerprint vs. facial recognition. ACM Computing Surveys, 56(4), 1-19. https://doi.org/10.1145/3600481

[12] Hernandez, J., & Ramirez, E. (2023). Investigating biometric attendance systems in higher education: Case studies in Latin America. IEEE Access, 11, 56733-56746. https://doi.org/10.1109/ACCESS.2023.3319564

[13] Kaur, G., & Singh, V. (2023). Integration of biometric systems into school discipline frameworks: Practical challenges and solutions. Springer Journal of Education and Information Technologies, 28(5), 745-758. https://doi.org/10.1007/s10639-023-11244-y

[14] Zhou, Q., & Li, Z. (2022). The impact of biometric systems on attendance tracking: A comparative analysis of public and private institutions. IEEE Transactions on Human-Machine Systems, 52(6), 1238-1248. https://doi.org/10.1109/THMS.2022.3112809

[15] Patel, A., & Kumar, N. (2023). Enhancing discipline through biometric systems in educational institutions: A case study of Indian universities. Elsevier Journal of Educational Computing Research, 59(6), 1123-1141. https://doi.org/10.1016/j.jecr.2023.104850

[16] Choudhury, A., & Verma, P. (2022). The future of biometric technology in educational security systems. ACM Transactions on Information Systems, 41(2), 34-45. https://doi.org/10.1145/3591249

[17] Zhang, L., Chen, Y., & Zhao, W. (2023). A hybrid approach to biometric systems in educational institutions: Combining facial and iris recognition. IEEE Transactions on Computational Social Systems, 9(5), 1786-1796. https://doi.org/10.1109/TCSS.2023.3298179

[18] Mohammed, Y., & Hassan, M. (2024). Biometric systems in fostering institutional discipline: A critical review. Springer Education and Information Technologies, 29(2), 283-298. https://doi.org/10.1007/s10639-023-11445-6

[19] Brown, K., & Davis, S. (2023). Exploring the role of biometric systems in maintaining student accountability. IEEE Transactions on Learning Technologies, 16(1), 245-257. https://doi.org/10.1109/TLT.2023.3167545

[20] Pires, R., & Almeida, F. (2023). Institutional discipline through biometric security: An analysis of Portuguese schools. Elsevier Computers & Education, 197, 104558. https://doi.org/10.1016/j.compedu.2023.104558

[21] Lee, C. H., & Kang, S. (2022). Fingerprint vs. iris recognition: A comparative study in educational settings. Journal of Applied Biometrics, 18(3), 302-312. https://doi.org/10.1016/j.japbiom.2022.05.004

[22] Nakamura, H., & Saito, T. (2023). Enhancing institutional discipline through the integration of biometric systems in Japan. IEEE Access, 11, 76789-76803. https://doi.org/10.1109/ACCESS.2023.3335672

[23] Fernandes, J., & Ramos, A. (2023). Security, efficiency, and biometric systems: Impact on school discipline in Europe. Elsevier Journal of Information Security and Applications, 74, 103221. https://doi.org/10.1016/j.jisa.2023.103221

[24] Diaz, M., & Gonzalez, L. (2024). Biometric time-tracking systems: Enhancing discipline in South American educational institutions. Springer International Journal of Educational Management, 32(1), 188-202. https://doi.org/10.1007/s10462-023-10829-4

[25] Khan, S., & Zaman, T. (2022). Adoption of biometric attendance systems in Pakistan's universities: Benefits and challenges. IEEE Transactions on Technology in Education, 64(3), 1230-1241. https://doi.org/10.1109/TE.2022.3024567