San Beda University
Mendiola, Manila

A Comparative Analysis of Automated Attendance Management Systems: Evaluating Accuracy, Efficiency, and Security

A Research submitted in partial fulfillment of
the requirement in the course
IT301: Research for IT

Submitted by:

ANINGALAN, Jul-Andrei T.
MAPULA, Paul Joshua G.
MARQUEZ, John Ariel A.

BIT3

ACKNOWLEDGEMENT

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

In today’s era, automated systems are becoming increasingly essential, not only because they improve efficiency by reducing the time spent on attendance tracking but also because they demonstrate the powerful synergy between human innovation and technology. These systems highlight the potential for reshaping the future of education through more advanced tools. Thus, switching to an automated system for monitoring attendance is a significant technological upgrade that has several advantages. Automated Attendance Management Systems (AMS) have emerged as efficient and reliable solutions to address these challenges. These systems leverage various technologies, such as fingerprint recognition, facial recognition, and RFID, to automate the attendance process, offering advantages in terms of accuracy, efficiency, and security.

Attendance management is a system for recording and maintaining student attendance, enabling universities to keep track of their students' time at their own respective institution. This system is essential for educational institutions as it helps monitor each student's progress and academic development. Accurate data in attendance is crucial for tracking student achievement, course credits, and ensuring compliance with institutional policies. Traditionally, student attendance is recorded through various procedures. In a classroom setting, professors often conduct roll calls, which consume valuable class time (Gornale & Kiran, 2020). Additionally, some schools still use handwritten logbooks for attendance. In contrast, non-manual procedures, such as using cards or RFID (Radio Frequency Identification), have been implemented in many schools to record attendance (Khan et al., 2019). However, the use of cards poses security risks, as students can use another student's card to gain entry to the school. These traditional procedures are often laborious, time-consuming, and prone to security risks, including the potential for falsified attendance records. With the rise of emerging technologies, one of the more efficient methods now under development is the application of biometrics (Nabi et al., 2023). Automated Attendance Management Systems are designed to streamline the process of tracking attendance by reducing human intervention and ensuring that records are maintained accurately and securely.

1.1 Statement of the Problem

Despite the growing adoption of AMS, a comprehensive understanding of the performance of these systems is still lacking, especially in terms of comparing the various technologies used and their impact on key performance metrics, such as accuracy, efficiency, and security. Thus, this study aims to fill this gap by providing a quantitative evaluation of various AMS technologies, focusing on their performance in the key areas of Accuracy, Efficiency, and Security. By synthesizing and analyzing data from previous studies, this research seeks to determine how these technologies compare and identify the strengths and weaknesses that organizations should consider when selecting an AMS.

1.2 Objectives

The primary objective of this study is to evaluate and compare the performance of different Automated Attendance Management Systems (AMS) based on three critical performance metrics: Accuracy, Efficiency, and Security. Specific objectives include:

1. Identify and review the various technologies used for attendance tracking based on accuracy, efficiency, and security.
2. To provide recommendations for the selection of AMS technologies, focusing on which technologies are best suited for specific performance requirements and contexts.

2. REVIEW OF RELATED LITERATURE

2.1 Automated Attendance Management Systems (AMS)

According to Aravindhan et al. (2021), attendance systems are used to monitor and manage attendance for various purposes, such as tracking student attendance at school or recording employee attendance in organizations. According to the study of Budiman (2023), the system can be manual, where individuals log in or mark their presence on a piece of paper, or automated, with technology such as biometric verification or facial recognition used to record attendance automatically. Automated attendance systems offer advantages such as accuracy, efficiency, and real-time data collection. They can integrate with other systems and provide easy access to attendance records for analysis and reporting purposes. Authentication systems are typically implemented in three main domains: time attendance and employee management systems, visitor management systems, authorization systems, and access control systems. Additionally, attendance systems have several characteristics, namely: Automatic Logging, Integration with Facial Recognition Technology, Log Maintenance, Biometric Authentication, Efficiency and Convenience, Non-Invasive Nature, and Application in Various Domains.

2.2 Performance Metrics of AMS

According to Anzar et al. (2021), the performance of AMS is generally evaluated based on three key metrics: Accuracy, Efficiency, and Security. These metrics are essential for assessing how well an AMS meets the needs of organizations and users. Each of these metrics is discussed in the following sections:

2.2.1 Accuracy

According to Singh et al. (2024), accuracy in AMS refers to the system's ability to correctly record the attendance of individuals without errors, such as false acceptances (where an unauthorized person is marked as present) or false rejections (where an authorized person is mistakenly marked absent). High accuracy is particularly important in educational settings, where attendance records have a direct impact on grading and administrative decisions.

According to the study of Ali et al. (2022), have shown that technologies like fingerprint recognition and facial recognition provide high accuracy levels. However, accuracy can vary across technologies, with some systems, like smartphone-based solutions, showing lower levels of reliability due to issues such as poor image quality or authentication failures.

2.2.2 Efficiency

According to Bavaskar et al. (2024), automated attendance systems are gaining traction due to their efficiency. Systems that require minimal setup time, have fast processing speeds, and are user-friendly contribute to higher efficiency. RFID-based systems, for instance, offer quick identification and attendance marking, often in a matter of seconds. In contrast, facial recognition systems may require more processing time, especially in environments with large numbers of users. Efficiency is a critical factor in environments where time is a limited resource, such as classrooms or corporate settings, where attendance tracking should not interfere with ongoing activities.

2.2.3 Security

Security in AMS refers to the protection of user data and the prevention of fraudulent activities such as identity theft or fake attendance logging. Systems that rely on biometric authentication, like the fingerprint-based attendance system in the study of Rahman et al. (2023), or facial recognition, are generally considered more secure than systems that use RFID or smartphone-based solutions. However, the security of biometric systems depends on the robustness of the technology and the security measures in place to protect the biometric data.

According to Anshari et al. (2021), addressing security issues is paramount to overcoming challenges and implementing an effective and efficient attendance system using facial recognition. Facial recognition systems, while highly accurate, can provide a reliable attendance solution by minimizing fraudulent activities and ensuring the authenticity of attendance logs. Nevertheless, they must address potential privacy concerns and ensure that the biometric data is safeguarded against cyber threats and unauthorized access. Similarly, smartphone-based systems, while convenient, may be susceptible to data breaches if not properly secured.

2.3 Types of AMS Technologies

According to Rjeib et al. (2018), various technologies are used in AMS to achieve different levels of performance in terms of accuracy, efficiency, and security. The following are some of the most widely adopted AMS technologies:

2.3.1 Fingerprint Recognition

Fingerprint recognition is one of the most established biometrics used in AMS. It is widely regarded as both accurate and secure, making it a popular choice for environments where security is a high priority. Several studies have shown that fingerprint-based systems can achieve high accuracy rates, with some systems reaching over 92% in accuracy like in the study of Saraswat & Kumar, (2010). Additionally, according to Kabir et al. (2021), fingerprint systems are generally fast and efficient, though they may struggle with issues such as worn or dirty fingers that could lead to false rejections. Despite these challenges, fingerprint recognition remains one of the most reliable AMS technologies.

2.3.2 Facial Recognition

According to the studies of Kortli et al. (2020) & Du et al. (2022), there are three basic steps are used to develop a robust face recognition system: First, *Face Detection* localizes human faces within an image, determining whether faces are present. Variations in lighting and expressions can interfere with detection, so preprocessing methods and tools like the Viola-Jones detector, HOG, PCA, and advanced deep learning techniques are used for this task. Second, *Feature Extraction* identifies distinctive facial features—such as the mouth, nose, and eyes—to create a "signature" based on geometry and structure. Finally, *Face Recognition* compares these features to a database to identify or verify individuals, using algorithms like K-nearest neighbor (K-NN) and Convolutional Neural Networks (CNN).

According to a study by Abir (2024), he designed and implemented an automated attendance management system using facial recognition technology. It uses a Convolutional Neural Network (CNN) model to identify and verify individuals based on their facial features. According to the study of Al-Nayyef (2024), a collected database of 800 images from 80 students is considered in his study. The images were taken using low-quality webcams in cell phones, laptops, etc. Each

student will be photographed more than once (five to ten times, depending on the gesture, lighting, perspective, and whether or not they are wearing glasses). The database is composed from a collection of 60 university students, and a collection from 20 young girls and boys taken from schools. Students' information such as student name, birth, email, class id, and so on, are stored in SQLite database.

2.3.3 Radio-Frequency Identification (RFID)

According to the study of Farag (2022), RFID technology is a widely utilized solution in automated attendance management systems (AMS), especially in environments where quick and contactless attendance tracking is essential. RFID systems rely on individuals carrying RFID tags or cards, which are scanned by an RFID reader to log attendance automatically. These systems are noted for their efficiency, as they can record attendance almost instantaneously, making them particularly suitable for settings that prioritize speed and convenience.

His study proposes a smart attendance system for students using RFID technology to enhance automation and convenience in school settings. The proposed RFID Attendance System (RFID-AS) is designed for implementation by school administrations to improve student safety, grading, and evaluation processes. Passive RFID technology was selected for its cost-effectiveness, and the system's main components include an RFID tag, an RFID reader, Visual Studio (utilizing the eXpressApp Framework tool), and an SQL Server. The system operates by comparing data from the RFID tag with the students' database to automatically log attendance. A graphical user interface (GUI) was also developed using Visual Studio to allow parents and school faculty to log in and review student attendance records. The process is streamlined, with students simply passing through a classroom door equipped with an integrated RFID reader to have their attendance recorded.

2.4 Comparative Studies on AMS

Several studies have investigated the implementation of various AMS technologies in different sectors. According to Ali et al. (2022), the majority of existing AMS implementations have been deployed in the academic sector, where attendance tracking is a critical component of

administrative processes. Additionally, AMS technologies have been utilized in other public and private settings, such as industries, organizations, and enterprises. From the comparative study, majority of these systems leverage biometric technologies, such as fingerprint recognition and facial recognition, due to their reliability and effectiveness in verifying individual identities. However, other AMS approaches, such as smartphone-based systems, web-based, and automated RFID systems, are also prevalent. RFID technology, in particular, has been widely used in academic and organizational settings due to its efficiency and ability to facilitate seamless attendance logging. In addition to RFID, other technologies like barcodes and smartcards have also been employed to enhance attendance management processes.

In the study of Basterretxea et al. (2024), a comparative analysis was conducted to evaluate the Type I error (α) rate of 10 post-hoc tests under varying conditions of heteroscedasticity and between-group sample size balance. Using a Monte Carlo simulation across 28 data sets with 10,000 resamples each, the study applied one-way ANOVA followed by post-hoc tests to assess the frequency with which the null hypothesis was falsely rejected at a 95% confidence level. These findings emphasized the importance of considering homoscedasticity and sample size balance in selecting appropriate post-hoc tests. While AMS systems are not the direct subject of this study, in his methodology, it highlights how rigorous statistical evaluation, such as ANOVA and post-hoc analysis, can be applied to compare performance metrics—similar to evaluating AMS technologies for accuracy, efficiency, and security.

3. METHODOLOGY

3.1 Research Design

This study adopts a quantitative research design to evaluate and compare the performance of various Automated Attendance Management Systems (AMS). The research is grounded in data collected and modified from Ali et al.'s (2022) systematic literature review, specifically Table 1: Critical Review of the Proposed AMS. By analyzing and refining the original data, this study focuses on understanding the relationships between different AMS technologies and their performance metrics: Accuracy, Efficiency, and Security.

3.2 Data Collection

The dataset for this study is sourced from Table 1: *Critical Review of the Proposed AMS* in Ali et al. (2022), which reviews 88 AMS implementations. The table summarizes the main findings for each study, serving as the foundation for extracting relevant metrics.

Table 1

Excerpt of the Critical Review of the Proposed AMS Table in Ali et al. (2022).

Author	Main Findings
Basheer and Raghu (2012)	Designed fingerprint-based attendance system and data management that has several advantages, such as automated management of attendance, prevents fake attendance registered and no time wasted when taking the attendance and absence of students.
Kassim et al. (2012)	RFID-based attendance system was proposed for academic field. This system aims to track students through their lecturers anywhere and anytime via accessible online system, improves teaching quality and monitors students' performance.
Benyo et al. (2012)	Introduced and developed an autonomous student attendance system through the NFC technology.
Venugopalan et al. (2012)	Introduced an effective automatic monitoring system (i.e. SickleSAM). This system monitors students' activities and attendance records daily, as well as the activities of adolescents with sickle cell disease to remove human bias and inaccuracies.
Othman et al. (2012)	Discussed the development of online attendance systems based on the concept of a web-based system architecture for higher academic institutions.

For instance, in the findings of Basheer and Raghu (2012) presented in table 1, the primary technology used was a fingerprint-based attendance system. The main findings emphasized its capability to prevent fake attendance registrations, which was mapped to a high level of accuracy. Additionally, the system's ability to eliminate time wasted during attendance-taking was interpreted as evidence of high efficiency. Furthermore, the prevention of fake attendance was also associated with a high-security rating. These interpretations allowed for the standardization of data extraction across the studies listed in the table.

Table 2

Excerpt of the Extracted AMS Dataset.

Author	Technology Used	Accuracy	Efficiency	Security
Basheer and Raghu (2012)	Fingerprint	High	High	High
Kassim et al. (2012)	RFID	High	High	Moderate
Benyo et al. (2012)	NFC	High	High	High
Venugopalan et al. (2012)	SickleSAM	High	High	Moderate
Othman et al. (2012)	Web-based	Moderate	High	Moderate

Note: Adapted from Ali et al. (2022), presenting an excerpt of the reviewed proposed AMS according to their main findings.

3.3 Data Preprocessing

The collected data was preprocessed to ensure consistency and prepare it for quantitative analysis. The preprocessing steps involved data cleaning, encoding categorical variables, and transforming the dataset into a format suitable for statistical analysis.

3.3.1 Data Cleaning

Non-standardized textual entries (such as "High; automates notifications") were cleaned to retain only the primary labels (e.g., "High") for the Accuracy, Efficiency, and Security columns.

3.3.2 Filtering Classes with Insufficient Representation

To ensure robust analysis and reduce the impact of underrepresented categories, technologies with only one instance in the dataset were excluded. This filtering step helped to focus the analysis on technologies with sufficient data to provide reliable insights.

3.3.3 Categorical Encoding

The performance metrics (Accuracy, Efficiency, and Security), originally represented as categorical values ("High", "Moderate", "Low"), were encoded into numerical values to facilitate quantitative analysis. The mapping was as follows:

- **High** = 3
- **Moderate** = 2
- **Low** = 1

This ordinal encoding process allows for the comparison of systems based on their relative performance in these metrics.

3.3.4 Handling Missing Data

In cases where data was missing, rows with incomplete entries were either excluded or imputed based on the frequency of similar data, ensuring minimal disruption to the dataset's integrity.

Table 3

Excerpt of the Pre-Processed AMS Dataset.

Author	Technology Used	Accuracy	Efficiency	Security
Basheer and Raghu (2012)	Fingerprint	3	3	3
Kassim et al. (2012)	RFID	3	3	2
Benyo et al. (2012)	NFC	3	3	3
Peter et al. (2013)	Fingerprint	3	3	3
Chintalapati and Raghunadh (2013)	Facial recognition	3	3	3

3.4 Statistical Analysis

The analysis of the data involved the following statistical techniques to evaluate the performance of Automated Attendance Management Systems (AMS):

3.4.1 Descriptive Statistics

Basic descriptive statistics were computed for the performance metrics: Accuracy, Efficiency, and Security. These statistics provided a general understanding of the dataset's central tendencies and variability. The mean ($\boldsymbol{\mu}$) was calculated using the formula:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

where $\boldsymbol{\mu}$ represents the mean, $\boldsymbol{n}$ is the total number of values, and x_i is each individual data point.

The standard deviation (σ) was then computed to measure the spread of the data points around the mean. The formula for standard deviation is:

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}$$

where σ is the standard deviation, x_i is each individual data point, **μ** is the mean, and ***n*** is the number of data points.

3.4.2 Correlation Analysis

A correlation matrix was generated to explore relationships among Accuracy, Efficiency, and Security. This analysis helped determine whether there were significant associations between the performance metrics and whether improvements in one metric corresponded to improvements or trade-offs in others. The Pearson Correlation Coefficient (r) was used to measure the strength of the linear relationship between two variables. The formula for Pearson's *r* is:

$$r = \frac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{\sqrt{[n\sum_{i=1}^{n} x_i^2 - (\sum_{i=1}^{n} x_i)^2][n\sum_{i=1}^{n} y_i^2 - (\sum_{i=1}^{n} y_i)^2]}}$$

Where r represents the correlation coefficient, x_i and y_i are the values of the two variables, and n is the number of data points. The formula helps quantify the degree to which the variables are related.

3.4.3 ANOVA (Analysis of Variance)

A one-way ANOVA (Analysis of Variance) was conducted to determine whether the means of Accuracy, Efficiency, and Security significantly differed across different AMS technologies. The ANOVA test compares the variance within groups (technology types) to the variance between groups. The F-statistic is calculated using the formula:

$$F = \frac{\text{Between-group variance}}{\text{Within-group variance}} = \frac{\frac{1}{k-1}\sum_{i=1}^{k} n_i(\bar{x}_i - \bar{x})^2}{\frac{1}{N-k}\sum_{i=1}^{k}\sum_{j=1}^{n_i}(x_{ij} - \bar{x}_i)^2}$$

Where ***F*** is the F-statistic, ***k*** is the number of groups (AMS technologies), n_i is the number of data points in the ***i***-th group, $\bar{x}$ is the mean of the ***i***-th group, and $\bar{x}$ is the overall mean of all data points. This test helped identify whether the choice of technology had a statistically significant impact on performance.

3.4.4 Tukey's Post Hoc Analysis

Tukey's HSD (Honestly Significant Difference) test was chosen as the post hoc analysis method due to its ability to compare all possible pairs of group means following significant results in the ANOVA. This method effectively controls the family-wise error rate, minimizing the risk of Type I errors (false positives) across multiple comparisons, while maintaining the specified significance level (e.g., α = 0.05). Tukey's HSD is particularly suitable for situations where the sample sizes across groups are equal or nearly equal, as it provides a robust and reliable means of identifying significant differences among multiple groups.

Additionally, According to Basterretxea et al. (2024), Tukey's HSD is well-suited for datasets that meet the assumption of homoscedasticity (equal variances), ensuring consistent and interpretable results. Its comprehensive approach to pairwise comparisons and its balance between Type I error control and statistical power make it an ideal choice for evaluating performance metrics in this study. The formula for Tukey's HSD is:

$$HSD = \frac{q_{\alpha,df,k} \cdot \sqrt{\frac{MS_{\text{within}}}{n}}}{\sqrt{2}}$$

Where $q\alpha, df_{error}$ is the studentized range statistic for a given significance level (α) and degrees of freedom for the error, MS_{error} is the mean square error from the ANOVA, and ***n*** is the number of observations per group.

4. RESULTS AND DISCUSSION

4.1 Descriptive Statistics

The descriptive analysis revealed that most systems achieved high accuracy, with a mean of 2.93 and minimal variability (standard deviation: 0.25), indicating consistent and reliable performance in delivering correct outputs. Similarly, efficiency was also consistently high, with a mean of 2.97 and very low variability (standard deviation: 0.18), reflecting well-optimized systems with uniform performance across different technologies. In contrast, security exhibited slightly more

variability, with a mean of 2.62 and a higher standard deviation of 0.49, suggesting that while some systems provided robust security measures, others offered only moderate levels. These findings indicate that accuracy and efficiency were strengths across the systems, showing minimal differences between technologies, whereas security varied more significantly, highlighting an area where improvements and standardization are needed.

Figure 1

Distribution of Accuracy, Efficiency, and Security Across Technologies.

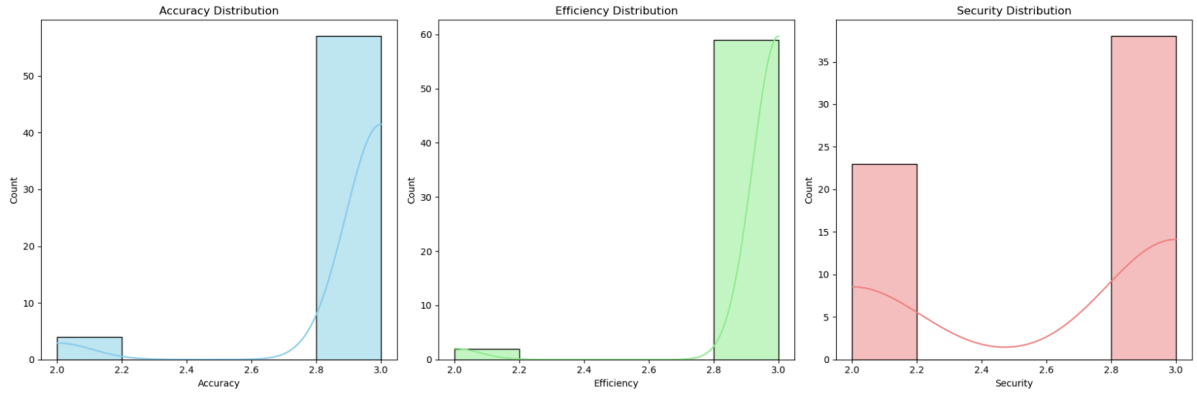
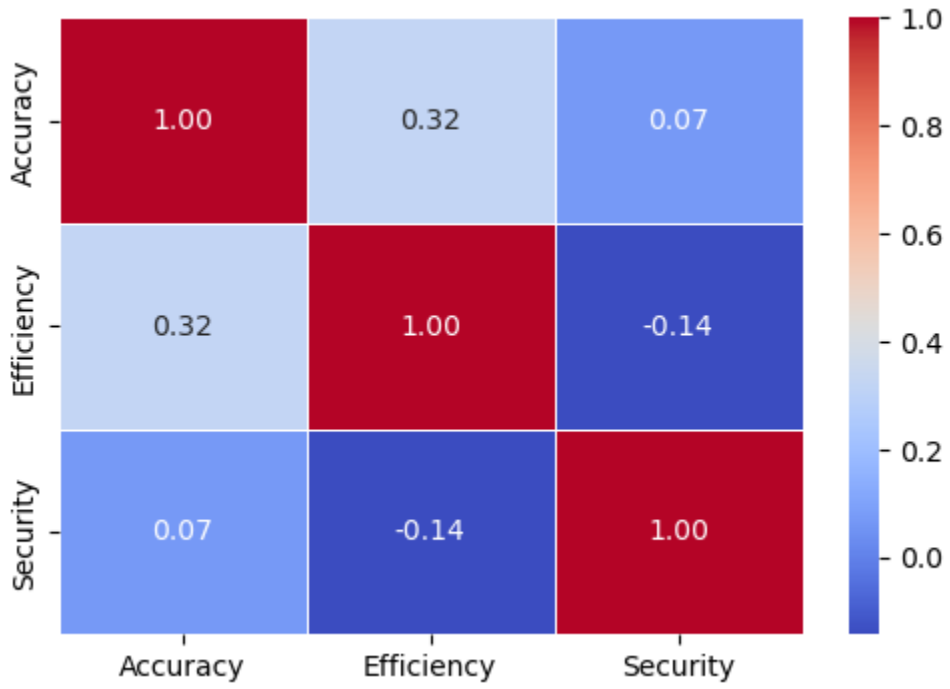


Figure 1 provides a detailed visualization of the descriptive statistics and distributions for three metrics: Accuracy, Efficiency, and Security. The analysis reveals that accuracy has a mean of 2.93 with a low standard deviation of 0.25, indicating high consistency across systems. The histogram shows a strong skew towards the maximum value of 3.0, with most systems clustering near this value, as confirmed by the density plot, which exhibits a sharp peak at 3.0. Similarly, efficiency demonstrates even greater consistency, with a mean of 2.97 and a standard deviation of only 0.18. The histogram and density plot show that most systems achieved the maximum value of 3.0, reflecting uniform high performance in this area. In contrast, security displays greater variability, with a mean of 2.62 and a standard deviation of 0.49. The histogram reveals a more dispersed distribution, with clusters around 2.0 and 3.0, and the density plot highlights a bimodal pattern, suggesting significant disparities in security levels across systems. Overall, while accuracy and efficiency are highly optimized and consistent, security shows notable variability, indicating a potential area for improvement and standardization.

4.2 Correlation Analysis

Figure 2

Correlation heatmap between Accuracy, Efficiency, and Security.



Note: The color intensity represents the strength of the correlation, with darker colors indicating stronger correlations.

Figure 2 shows the correlations between Accuracy, Efficiency, and Security, with the intensity of colors reflecting the strength of these relationships. The diagonal entries, which are all equal to 1.00, represent the perfect self-correlation of each metric. The off-diagonal elements highlight the relationships between different metrics.

A moderate positive correlation (0.32) is observed between Accuracy and Efficiency, implying that systems with higher accuracy tend to also exhibit better efficiency, though the relationship is not particularly strong. In contrast, Security shows very weak correlations with both Accuracy (0.07) and Efficiency (-0.14). This suggests that security performance is largely independent of improvements in the other two metrics, indicating that accuracy and efficiency optimizations do not necessarily enhance security.

The weak or negligible correlations involving Security highlight the need to address security separately, as it does not inherently align with the trends seen in accuracy and efficiency. The heatmap effectively captures these relationships and serves as a visual guide for prioritizing improvements in areas that may require independent focus.

4.3 ANOVA Results

The One-Way ANOVA analysis was conducted to assess the differences in Accuracy, Efficiency, and Security among the various technologies used for AMS systems.

Based on the results, the ANOVA test for Accuracy showed a statistically significant difference among the technologies ($F = 2.84$, $p = 0.018$). This suggests that the technology used has an impact on the accuracy of the system. However, the post-hoc analysis using Tukey's HSD test revealed no significant differences between any specific technology pairs. While the overall ANOVA result indicates a difference, the individual technologies in the study perform similarly in terms of accuracy.

In terms of efficiency, it showed no significant differences among the technologies ($F = 0.41$, $p = 0.870$). This result indicates that the technology used does not significantly impact the efficiency of the system, suggesting that all technologies in the study perform similarly in terms of efficiency.

For security, the ANOVA test showed a highly significant difference across technologies ($F = 12.21$, $p < 0.001$). This indicates that the technology used plays a critical role in the security of the system. The post-hoc analysis using Tukey’s HSD test revealed that Smartphone-based systems exhibited significantly lower security compared to technologies such as RFID, Facial Recognition, and Fingerprint systems.

4.4 Post Hoc Analysis (Tukey’s HSD)

Table 4

Post Hoc Tukey HSD Test Results for Accuracy

Multiple Comparison of Means - Tukey HSD, FWER=0.05

group1	group2	meandiff	p-adj	lower	upper	reject
Facial recognition	Fingerprint	0.0588	0.9941	-0.213	0.3306	False
Facial recognition	NFC	0.0588	0.9987	-0.2985	0.4162	False
Facial recognition	RFID	0.0588	0.9914	-0.1947	0.3123	False
Facial recognition	Smart card	-0.4412	0.1549	-0.9662	0.0839	False
Facial recognition	Smartphone	-0.0412	0.9993	-0.3211	0.2387	False
Facial recognition	Speech recognition	-0.4412	0.1549	-0.9662	0.0839	False
Fingerprint	NFC	0.0	1.0	-0.3788	0.3788	False
Fingerprint	RFID	0.0	1.0	-0.283	0.283	False
Fingerprint	Smart card	-0.5	0.0867	-1.0399	0.0399	False
Fingerprint	Smartphone	-0.1	0.9523	-0.4069	0.2069	False
Fingerprint	Speech recognition	-0.5	0.0867	-1.0399	0.0399	False
NFC	RFID	0.0	1.0	-0.3659	0.3659	False
NFC	Smart card	-0.5	0.1447	-1.0877	0.0877	False
NFC	Smartphone	-0.1	0.9844	-0.4847	0.2847	False
NFC	Speech recognition	-0.5	0.1447	-1.0877	0.0877	False
RFID	Smart card	-0.5	0.0774	-1.031	0.031	False
RFID	Smartphone	-0.1	0.9388	-0.3908	0.1908	False
RFID	Speech recognition	-0.5	0.0774	-1.031	0.031	False
Smart card	Smartphone	0.4	0.2865	-0.1441	0.9441	False
Smart card	Speech recognition	0.0	1.0	-0.7024	0.7024	False
Smartphone	Speech recognition	-0.4	0.2865	-0.9441	0.1441	False

Table 5

Post Hoc Tukey HSD Test Results for Security

Multiple Comparison of Means - Tukey HSD, FWER=0.05

group1	group2	meandiff	p-adj	lower	upper	reject
Facial recognition	Fingerprint	-0.0321	1.0	-0.4296	0.3655	False
Facial recognition	NFC	-0.1412	0.981	-0.6639	0.3815	False
Facial recognition	RFID	-0.5126	0.0017	-0.8834	-0.1418	True
Facial recognition	Smart card	0.0588	1.0	-0.7092	0.8269	False
Facial recognition	Smartphone	-0.9412	0.0	-1.3506	-0.5317	True
Facial recognition	Speech recognition	-0.9412	0.0074	-1.7092	-0.1731	True
Fingerprint	NFC	-0.1091	0.9965	-0.6632	0.445	False
Fingerprint	RFID	-0.4805	0.0132	-0.8945	-0.0666	True
Fingerprint	Smart card	0.0909	0.9998	-0.6989	0.8807	False
Fingerprint	Smartphone	-0.9091	0.0	-1.358	-0.4602	True
Fingerprint	Speech recognition	-0.9091	0.0144	-1.6989	-0.1193	True
NFC	RFID	-0.3714	0.3534	-0.9067	0.1638	False
NFC	Smart card	0.2	0.9913	-0.6596	1.0596	False
NFC	Smartphone	-0.8	0.0011	-1.3627	-0.2373	True
NFC	Speech recognition	-0.8	0.0839	-1.6596	0.0596	False
RFID	Smart card	0.5714	0.2856	-0.2052	1.3481	False
RFID	Smartphone	-0.4286	0.0472	-0.854	-0.0032	True
RFID	Speech recognition	-0.4286	0.6256	-1.2052	0.3481	False
Smart card	Smartphone	-1.0	0.0055	-1.7958	-0.2042	True
Smart card	Speech recognition	-1.0	0.0613	-2.0274	0.0274	False
Smartphone	Speech recognition	0.0	1.0	-0.7958	0.7958	False

As shown in table 1, there are no significant differences observed between any of the technology pairs. This finding suggests that while Accuracy showed a significant difference across the technologies in the ANOVA, the actual differences between individual technologies are not substantial enough to be considered statistically significant.

For security, results in Tukey's HSD are shown in table 2, there are several significant differences between technology pairs, indicating that security performance varies considerably across different AMS technologies. Facial recognition exhibited significantly higher security compared to Smartphone (p-adj = 0.0000), RFID (p-adj = 0.0017), and speech recognition (p-adj = 0.0074). Fingerprint systems also showed significantly better security compared to smartphone (p-adj = 0.0000), RFID (p-adj = 0.0132), and speech recognition (p-adj = 0.0144). On the other

hand, smartphone-based systems showed significantly weaker security than RFID (p-adj = 0.0472), Facial recognition (p-adj = 0.0000), and Fingerprint (p-adj = 0.0000).

These findings suggest that Smartphone-based systems tend to be more vulnerable to security risks, possibly due to issues related to mobile application frameworks and security protocols. Technologies like Facial recognition and Fingerprint performed significantly better in terms of security, making them preferable choices for environments where security is a top priority.

4.5 Discussion of Findings

The analysis revealed that most technologies, such as Fingerprint and NFC, consistently performed well across all metrics, demonstrating high accuracy and efficiency with minimal variability. These technologies are reliable choices for AMS systems, offering robust performance and a balance of precision and optimization. Smartphone-based systems, however, did not exhibit any significant advantages in terms of accuracy or efficiency, suggesting that they might not be the best choice for AMS applications where these attributes are critical.

Security performance varied considerably across the technologies evaluated. Smartphone-based systems displayed significant weaknesses in this area, likely due to inherent vulnerabilities in mobile application frameworks, insufficient encryption protocols, and exposure to a wider range of cyber threats. Conversely, technologies such as Fingerprint, RFID, and Facial Recognition demonstrated robust security performance, making them more suitable for environments where security is a top priority.

Organizations prioritizing security should carefully consider the technology they adopt. Smartphone-based systems, while offering portability and ease of use, are not ideal for high-security environments due to their weaker security performance. Fingerprint and NFC technologies emerge as strong candidates for organizations seeking reliable accuracy and efficiency across AMS systems, providing consistent performance with minimal variability. Facial Recognition technology, while highly secure and effective, should also be considered a leading option, particularly in scenarios requiring hands-free operation or where biometrics are essential for identification. However, the potential for ethical concerns, such as privacy

violations or biases in recognition, must be carefully managed to ensure responsible deployment. For environments that demand both security and accessibility, Facial Recognition, along with Fingerprint systems, represents a highly effective solution.

4.6 Limitations and Future Work

The study's findings provide valuable insights into the performance of various AMS technologies across accuracy, efficiency, and security metrics. However, certain limitations must be acknowledged. First, the dataset size was a key constraint, particularly for some technologies with fewer instances. This limitation may have restricted the generalizability of the findings and the ability to draw stronger conclusions. A larger dataset encompassing more diverse and representative samples could improve the robustness and reliability of the analysis.

Another limitation is that the study did not account for context-specific factors, such as geographic location, user demographics, or organizational environments, which could influence the performance of the technologies. For example, user preferences or cultural norms might impact the adoption and effectiveness of certain technologies, such as Facial Recognition or Smartphone-based systems.

Future research should address these limitations by expanding the dataset to include more comprehensive and diverse instances of AMS technologies. Furthermore, exploring additional performance metrics, such as user satisfaction, cost-effectiveness, and ease of integration, could provide a more holistic understanding of the strengths and weaknesses of different systems. Another promising avenue for future work involves assessing the long-term reliability and scalability of these technologies in real-world scenarios. Incorporating qualitative analyses, such as user feedback and case studies, could also shed light on the practical challenges and benefits associated with the deployment of AMS technologies.

5. CONCLUSION AND RECOMMENDATIONS

In conclusion, this study has provided a comprehensive evaluation of various Automated Attendance Management Systems (AMS) by examining their performance across three critical metrics: Accuracy, Efficiency, and Security. The findings indicate that while most AMS technologies, such as Fingerprint and NFC, demonstrated high accuracy and efficiency with minimal variability, security varied significantly among the technologies. Smartphone-based systems were found to exhibit notable weaknesses in security, while systems like Fingerprint, RFID, and Facial Recognition performed better in this regard, making them more suitable for environments where security is a top priority.

Based on the research objectives, the study successfully compared the various AMS technologies and identified the strengths and weaknesses of each. The results suggest that technologies like Fingerprint and NFC are reliable for AMS applications that prioritize accuracy and efficiency. However, for environments requiring heightened security, technologies like Facial Recognition and Fingerprint offer substantial advantages.

Given the limitations of the study, including the relatively small dataset and the absence of context-specific factors, future research should focus on expanding the dataset to include more diverse AMS implementations and explore additional performance metrics, such as user satisfaction and cost-effectiveness. Moreover, incorporating real-world case studies and qualitative feedback could further enhance the understanding of AMS technologies' practical applications. Addressing these gaps will provide a more robust and holistic perspective on the most suitable AMS technologies for different environments.

REFERENCES

Abir, A. (2024). Automated attendance management system using Face Recognition (CNN). Theseus. https://urn.fi/URN:NBN:fi:amk-2024060621631.

Ali, N. S., Rjeib, H. D., Alsharqi, H., & Al-Sadawi, B. (2022). Automated attendance management systems: systematic literature review. International Journal of Technology Enhanced Learning, 14(1), 37-65. https://doi.org/10.1504/IJTEL.2022.120559.

Al-Nayyef, H. (2024). Advancing Attendance: A Facial Recognition System Empowered by Deep Learning Techniques. Journal of Al-Qadisiyah for Computer Science and Mathematics, 16(1), 61–71 . https://doi.org/10.29304/jqcsm.2024.16.11435.

Anshari, A., Hirtranusi, S. A., Sensuse, D. I., Kautsarina, & Suryono, R. R. (2021). Face Recognition for Identification and Verification in Attendance System: A Systematic Review. IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), 316-323. https://doi.org/10.1109/COMNETSAT53002.2021.9530817.

Anzar, S. M., Subheesh, N. P., Panthakkan, A., Malayil, S., & Ahmad, H. A. (2021). Random Interval Attendance Management System (RIAMS): A Novel Multimodal Approach for Post-COVID Virtual Learning. IEEE Access, 9(1), 91001-91016. https://doi.org/10.1109/ACCESS.2021.3092260.

Aravindhan, K., Sangeetha, S. K. B., Periyakaruppan, K., Keerthana, K. P., SanjayGiridhar, V., & Shamaladevi, V. (2021). Design of Attendance Monitoring System Using RFID. 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 1628-1631. https://doi.org/10.1109/ICACCS51430.2021.9441704.

Basterretxea, J. J., Diego, G. A., Postigo, A., Alvarez, P. M., Aller, A. M., & Cueto, E. G. (2024). Post-Hoc Tests in One-Way ANOVA: The Case for Normal Distribution. Methodology, 20(2), 84-99. https://doi.org/10.5964/meth.11721.

Budiman, A., Fabian, Yaputera, R. A., Achmad, S., Kurniawan, A. (2023). Student attendance with face recognition (LBPH or CNN): Systematic literature review. Procedia Computer Science, 216(1), 31-38. http://dx.doi.org/10.1016/j.procs.2022.12.108.

Bavaskar, V., Sontakke, P., & Wadode, H. (2024). Face Recognition Attendance System. Sant Gadge Baba Amravati University, Amravati. Dissertation.

Farag, W. A. (2022). An RFID-based Smart School Attendance and Monitoring System. BOHR International Journal of Computational Intelligence and Communication Network, 1(1), 26-34. https://doi.org/10.54646/bijcicn.005.

Gornale, B., & Kiran, P. (2020). *Classroom Attendance Management System Using Camera*. International Journal of Research in Engineering, Science and Management, 3(8), 327-330. https://journal.ijresm.com/index.php/ijresm/article/view/191

Kabir, H., Roy, S., Ahmed, T., & Alam, M. (2021). Smart Attendance and Leave Management System Using Fingerprint Recognition for Students and Employees in Academic Institute. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 10(6), 268-279.

Khan, M. Z., Harous, S., Hassan, S. U., Khan, M. U. G., Iqbal, R. & Mumtaz, S. (2019). *Deep Unified Model For Face Recognition Based on Convolution Neural Network and Edge Computing*. IEEE Access. PP. 1-1. https://doi.org/10.1109/ACCESS.2019.2918275

Kortli, Y., Jridi, M., Falou, A. & Atri, M. (2020). Face Recognition Systems: A Survey. Sensors, 20(2), 342. https://doi.org/10.3390/s20020342.

Nabi, M. S., Mohiuddin, G., Mfaki, Z. & Abdullahi, A. M. (2023). *A Comprehensive Face Recognition Solution for Attendance and Social Security System Using CNN*. Malaysian Journal of Information and Communication Technology (MyJICT), 8(2), 8-22. https://doi.org/10.53840/myjict8-2-29

Rahman, S., Rumman, K. M., Ahmmed, R., Rahman, A., & Sarker, A. (2023). FINGERPRINT BASED BIOMETRIC ATTENDANCE SYSTEM. European Chemical Bulletin, 12(1), 184-190. https://doi.org/10.31838/ecb/2023.12.s3.026.

Rjeib, H. D., Ali, N. S., Al Farawn, A., Al-Sadawi, B. and Alsharqi, H. (2018). Attendance and information system using RFID and web-based application for academic sector, International Journal of Advanced Computer Science and Applications, 9(1), 266–274. http://dx.doi.org/10.14569/IJACSA.2018.090137.

Saraswat, C. & Kumar, A. (2010). An Efficient Automatic Attendance System using Fingerprint Verification Technique. (IJCSE) International Journal on Computer Science and Engineering, 2(2), 264-269.

Singh, J., Majumdar, K., Singh, N., Gupta, C., Banda, L., & Jain, K. (2024). A systematic review and research perspective on Attendance Management System. Journal of Applied Optics. https://doi.org/10.31219/osf.io/2ptky.