FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 12, December, 2025, pp 126 – 131
DOI: https://doi.org/10.33003/fjs-2025-0912-4244

ANALYSIS OF USING BIOMETRIC AUTHENTICATION SYSTEM IN KATSINA STATE INSTITUTE OF TECHNOLOGY AND MANAGEMENT (KSTIM) LIBRARY

***[1]Maryam Sani and [2]Umar Abba**

[1]Department of Networking and System Security, Katsina State Institute of Technology and Management, Katsina State, Nigeria.
[2]Department of Computer Science, Katsina State Institute of Technology and Management, Katsina State, Nigeria.

*Corresponding authors' email: sanimaryam9@gmail.com Phone: +2348039778834

ABSTRACT

This research investigates the feasibility and benefits of implementing biometric authentication in the Katsina State Institute of Technology and Management (KSITM) Library, emphasizing its potential to enhance security and safeguard sensitive information. Traditional methods, like passwords and tokens, are vulnerable as they can be easily shared or compromised, often leading to security lapses. Biometrics, however, provide a more secure solution by using unique physical characteristics, such as fingerprints, hand geometry, palm veins, retina and iris patterns, facial recognition, signature, and voice analysis, to accurately verify individual identities. The study reviews these biometric methods, assessing their usability, advantages, and potential drawbacks. A questionnaire-based approach was used to gauge the satisfaction and receptiveness of KSITM's staff and students toward biometric systems. Findings show that 85% of respondents consider biometric authentication an essential improvement for the library, demonstrating a strong preference for it over traditional methods. Respondents showed the highest preference for fingerprint recognition, favoring its balance of convenience, security, and reliability. This feedback suggests that implementing a biometric system could enhance the library's security infrastructure and reduce the risks associated with traditional access methods. Overall, the positive response indicates that biometric authentication is both a viable and beneficial security measure for KSITM, fostering a more secure and controlled environment for students and staff.

Keywords: Biometrics, Authentication, Security, Password

INTRODUCTION

Authentication plays a crucial role in security by verifying the identity of individuals, systems, or devices. With the rise of international regulations and evolving technology, new methods for securing information and confirming identities have emerged. Among these, biometrics has become a leading solution due to its ability to reliably and quickly identify individuals based on their unique physical traits, such as fingerprints, facial recognition, or iris scans(Byron et al., 2021).

A biometric or biometric identifier refers to the objective measurement of a person's physical or behavioral characteristic, such as a fingerprint, facial pattern, iris, or voice. Once captured and stored in a database, this information can be used to verify an individual's identity by comparing it to a previously recorded entry, or to check it against other stored entries for identification purposes(Phadke, 2013). Biometric identifiers provide a high level of security because they are unique to each person and difficult to forge or duplicate. This makes them a reliable means of authentication in various systems, from personal devices to large-scale security infrastructures. When properly implemented, biometrics offer not only increased security but also convenience, as users no longer need to remember passwords or carry physical tokens. However, the secure storage and handling of biometric data are critical, as misuse or theft of such data can have serious privacy and security implications.

Biometric authentication is more secure than traditional methods because it relies on intrinsic characteristics of a person, which are difficult to replicate or forge. As regulations evolve to address growing security threats, biometrics continues to gain prominence for its efficiency, accuracy, and security in various applications, from personal devices to critical infrastructure. Its increasing adoption demonstrates its effectiveness in meeting the demands of modern security challenges while aligning with regulatory frameworks that emphasize the protection of sensitive information.

Biometric authentication leverages an individual's unique biological traits to confirm their identity and provide secure access to electronic systems. These technologies rely on the fact that each person has distinct physical or behavioral characteristics, making them highly reliable for identity verification. Common biometric traits used in authentication include:

i. Fingerprint: Unique ridge patterns on the fingers.
ii. Hand morphology: The shape and size of the hand.
iii. Retina and iris: Distinct patterns in the eye.
iv. Voice: Specific vocal patterns unique to each person.
v. DNA: The most unique identifier, though less commonly used in everyday systems.
vi. Signatures: Behavioral patterns in the way a person signs their name.

These biometric systems offer significant security advantages by making it difficult for unauthorized users to replicate or steal someone's biological data. This type of authentication is increasingly adopted for personal devices, financial systems, and even in border control due to its accuracy and convenience (Albalawi et al., 2022).

MATERIALS AND METHODS

Related Literatures

With the rapid rise in electronic crimes and their associated risks, the need for reliable user authentication systems has become essential for ensuring both access control and the protection of private data. Human biometric characteristics, such as facial recognition, fingerprints, iris scans, voice patterns, and signatures, provide a high level of security for both personal and public applications. Biometric

authentication systems have been in use for a considerable time, with their effectiveness rooted in the uniqueness of each individual's biological traits, which plays a key role in reducing the success of imposter attacks. Unlike traditional security methods such as passwords or PINs, which can be easily forgotten, stolen, or hacked, biometric systems offer more robust protection due to their inherent uniqueness. This paper focuses on the concept of psychological biometric authentication techniques**,** which refers to methods of identifying individuals based on behavior-related characteristics, adding another layer of security in authentication processes. These systems represent a significant improvement over older methods, providing better security against unauthorized access and reducing the risk of electronic crimes (Israa M. Alsaadi, 2012).

Advancements in the accuracy, usability, and affordability of biometric technology have made it a highly secure, cost-effective solution for identifying individuals. Biometric modalities like fingerprint scanning, retinal and iris scanning, signature verification, hand geometry, and voice recognition are well-established, each with unique strengths. These technologies are now widely used in both public and private sectors due to their reliability and enhanced precision. Limitations that previously impacted the adoption of biometrics, such as speed and bandwidth, have largely been overcome. As a result, biometric systems can now perform better than expected in many scenarios, making them an even more practical and scalable solution for secure authentication. This has contributed to their growing use in everything from smartphones and laptops to border security and financial services. As these technologies continue to improve, they offer greater security while remaining efficient and accessible for a wide range of applications (Pujari et al., 2021).

Today, various security and business procedures depend heavily on the automatic recognition of individuals, with biometric recognition playing a crucial role. Biometric recognition refers to the process of identifying or verifying a person based on the analysis of their unique physiological or behavioral characteristics. While highly effective, no biometric system is 100% accurate or flawless. Each biometric method whether it be fingerprinting, facial recognition, or iris scanning has its own strengths and weaknesses(Majeed Alsaadi, 2021). A comprehensive study has been conducted to review the most commonly used biometric technologies for personal identification. Future research in this area will involve an in-depth investigation of multiple biometric techniques and the algorithms that power them. Additionally, a comparative study is necessary to analyze these systems in detail, providing valuable insights for security researchers to better understand the performance, reliability, and limitations of various biometric methods(Majeed Alsaadi, 2021).

Securing sensitive information has long been a critical focus, with authentication methods evolving over time. Historically, passwords were the primary tool, but they posed risks as people often used predictable, easy-to-guess passwords or wrote them down for fear of forgetting them. Although password complexity and two-factor authentication (2FA) have improved security, vulnerabilities still exist. To address these issues, biometric authentication methods such as fingerprints, facial recognition, and iris scans have become more prevalent. Biometrics offer a more secure and convenient alternative to passwords, eliminating the need to remember or type credentials. However, while biometrics enhance security, they are not entirely immune to hacking. As hackers develop new methods to bypass biometric systems, the industry continues to face challenges in ensuring foolproof protection. Therefore, while biometrics reduce many risks, continuous advancements and vigilance are necessary to maintain strong defenses against emerging threats (Kamble et al., 2024).

Types of Biometric Authentications

Fingerprint

Fingerprints are indeed a popular biometric identifier because of their uniqueness and convenience in securing devices such as smartphones, tablets, and laptops. Unlike traditional passwords or PINs, which can be forgotten or stolen, biometric data like fingerprints are inherent to the individual and can't be easily replicated or lost. This makes them a stronger security measure, as well as a faster and more user-friendly method for unlocking devices or authenticating identity.

However, while biometrics offer significant advantages in terms of security and convenience, there are concerns about privacy and the irreversible nature of biometric data. Once compromised, a fingerprint can't be changed like a password, which introduces different types of risks in the realm of information security (Weaver, 2006). Nonetheless, the integration of biometric authentication continues to grow due to its practical benefits but Fingerprint recognition is generally it's considered as reliable enough for commercial use, and some vendors are already actively marketing readers as part of Local Area Network login schemes [Phadke, 2013].

Hand morphology

The essence of hand geometry is the comparative dimensions of fingers and the locations of joints. One of the earliest automated biometric systems, Indent mat, installed at the Shearson-Hamill investment bank on Wall St. during the late 60s, used hand geometry and stayed in production for almost twenty years. Some systems perform simple, two-dimensional measurements of the palm of the hand. Others attempt to construct a simple three-dimensional image from which to extract template characteristics. [Wayman, 2001].

Figure 1: Hand Geometry [DALL-E Image Creation]

Retinal Scan

Retina-based biometric authentication relies on the unique pattern of blood vessels in the retina at the back of the eye. Each person's retinal pattern is distinct and different from others. Since the retina is not directly visible, an infrared light source is used to illuminate it. Blood vessels absorb infrared light more quickly than the surrounding tissue, creating a contrast that allows for the detailed imaging and analysis of the retinal blood vessel pattern. This method provides a highly secure form of identification due to the uniqueness of retinal patterns (Weaver, 2006).

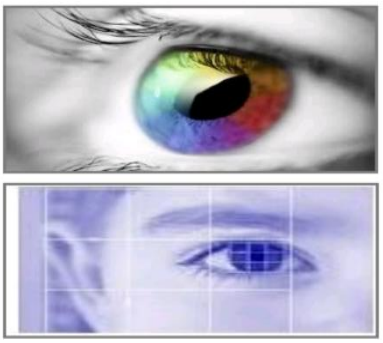

Figure 2: Retinal Scan [Phadke, 2013]

Voice

Voice recognition techniques are generally categorized according to two approache's Automatic Speaker Verification (ASV) and Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario. Speaker identification attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual's voice at enrollment time, and more than one enrolment session is often necessary. Feature extraction typically measures formants or sound characteristics unique to each person's vocal tract. The pattern matching algorithms used in voice recognition are similar to those used in face recognition.

Figure 3: Voice [Phadke, 2013]

Iris

Iris scanning is less intrusive than retinal recognition because the iris is easily visible from several feet away. Responses of the iris to changes in light can provide secondary verification that the iris presented as a biometric factor is genuine. Though empirical tests with the technology will improve its reliability, it appears quite promising and even practical for many applications, especially two-factor scenarios [Wayman, 2001].

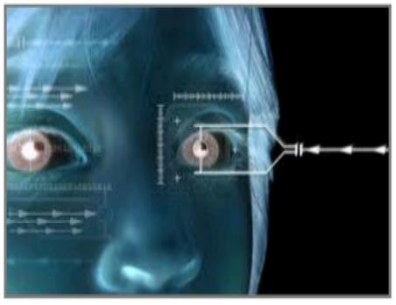

Figure 4: Iris [Phadke, 2013]

Face/Facial Thermo Gram

Facial recognition is a biometric technique used to identify or verify individuals based on their facial features, utilizing photos or video recordings. The process typically involves four key steps:

i. Facial Detection: Identifying and locating the human face within an image.
ii. Feature Extraction: Extracting distinctive feature vectors from the detected face, which is the most critical step in the process.
iii. Feature Classification: Classifying the extracted features based on predefined criteria.
iv. Feature Matching: Comparing the classified features with those in a database to determine identity.

Each step plays a crucial role in ensuring accurate facial recognition, with feature extraction being particularly vital for the system's robustness and effectiveness (Byron et al., 2021).

Figure 5: Face/Facial TI [DALL-E Image Creation]

Hand Vein

Hand vein recognition attempts to distinguish individuals by measuring the differences in subcutaneous features of the hand using infrared imaging. Like face recognition, it must deal with the extra issues of three-dimensional space and the orientation of the hand. Like retinal scanning, it relies on the pattern of the veins in the hand to build a template with which to attempt matches against templates stored in a database. The use of infrared imaging offers some of the same advantages as hand geometry over fingerprint recognition in manufacturing or shop-floor applications where hands may not be clean enough to scan properly using a conventional video or capacitance technique.

Figure 6: Hand Vein [Phadke, 2013]

Signature

Signature dynamics recognition analyzes the process of signing by measuring factors like pressure, direction, acceleration, stroke length, and duration. This method offers enhanced security since fraudsters can't replicate the dynamic aspects of the signing process just by observing a static signature. Special pens and tablets capture these dynamics, but tablets can present challenges, such as producing a different digital signature and requiring users to view the monitor rather than the paper. Some pens combine ink cartridges with dynamic capture, but overall accuracy is limited, with manufacturers reporting a crossover rate of around 2% and practical accuracy often being lower (Kamble et al., 2024).

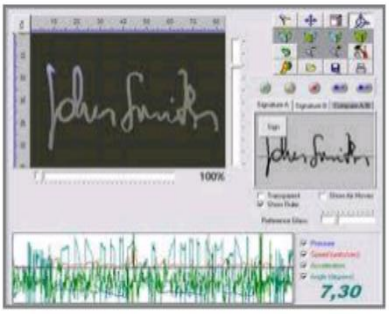

Figure 7: Signature [Phadke, 2013]

DNA

The DNA is an acronym for deoxyribonucleic acid which is present in nucleus of every cell in human body and therefore a highly stable biometric identifier that represents physiological characteristic. The DNA structure of every human is unique, except from identical twins, and is composed of genes that determine physical characteristics (like eye or hair color). Human DNA samples can be acquired from a wide variety of sources; from hair, finger nails, saliva and blood samples. Identification based on DNA requires first isolating from source/samples, amplifying it to create multiple copies of target sequence, followed by sequencing that generates a unique DNA profile **(**Phadke, 2013).

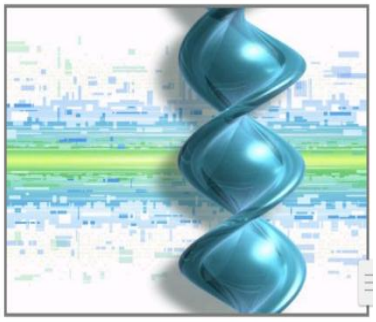

Figure 8: DNA [Phadke, 2013]

Ear Recognition

Another biometric authentication method focuses on recognizing the unique shape and appearance of a person's ear. Unlike many other body parts, the human ear maintains a consistent visual shape throughout a person's life, even as they grow and age. This stability makes ear-based recognition a dependable and secure option for identifying or verifying individuals. The fact that the ear does not change significantly over time enhances its reliability as a biometric identifier, offering a promising alternative for secure authentication in various applications (Kamble et al., 2024).

Methodology

The research employs a structured questionnaire methodology to gather quantitative data on the attitudes, preferences, and satisfaction levels of KSITM students and staff regarding biometric authentication in the library. The questionnaire consists of closed-ended questions that capture specific metrics such as agreement with the importance of biometric systems, satisfaction with current security measures, and preferences among various biometric methods (e.g., fingerprint, hand geometry, voice recognition). Additionally, Likert scale questions will assess the strength of respondents' views on biometric security benefits and potential privacy concerns. To ensure diverse participation, the questionnaire was distributed both online and in person, targeting a representative sample across different departments and user roles in the library. This approach allows for a systematic analysis of trends and comparisons between subgroups, providing insight into the most favored biometric system and the general receptivity to its implementation.

RESULTS AND DISCUSSION

The data collected from the respondents was analyze and the result is presented below. There are six (6) questions in the questionnaire the respondents are expected to answer carefully by supporting their answers with reason.

The results of the analysis are presented in the table and chart below:

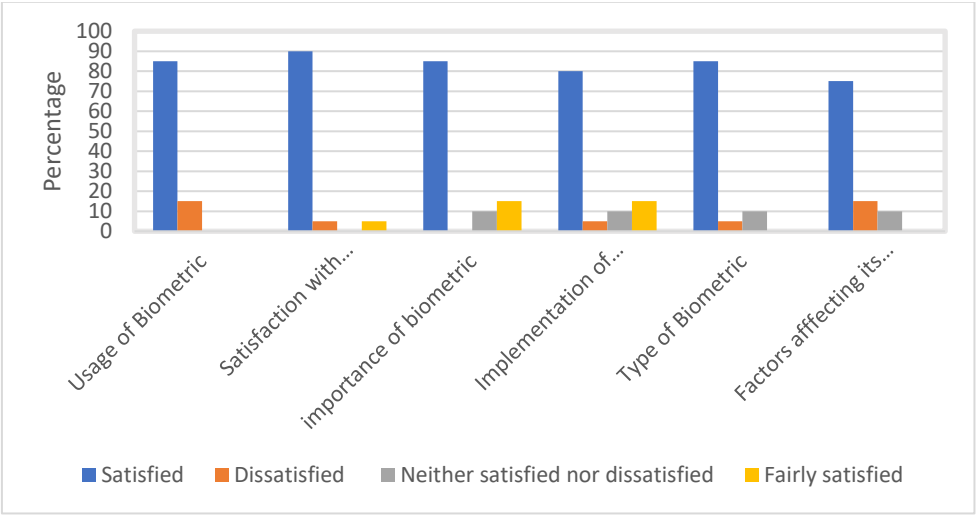

Figure 10: Result of the Analysis

The data revealed that more than 95% of the staff and student have positive attitude toward biometric authentication to build more security in the school library that support their studies. Although the issue is based on what the student and staffs respond about their satisfaction of biometric authentication in different places, the result shows that the student and staff are interest in implementing biometric authentication in the

Katsina State Institute of Technology and Management (KSITM) Library.

According to the analysis, the 85% of the respondent who took part in the analysis Agreed and satisfied with important of biometric authentication where the 15% somewhat satisfied with the idea. At the other hand, 75% believed that there are factors align with the biometric authentications. Also, 90% of the respondents are very satisfied and welcoming biometric authentication and 80% agreed if the school management implement the idea in the school library it will result into a proper management. Furthermore, 85% of the respondents took fingerprint as their opinion if the Institute will implement the biometric authentication in their library where 10% took hand geometry and only 5% take voice recognition.

Finally, the review shows strong support among staff and students for implementing biometric authentication in the KSITM library, with over 95% expressing positive attitudes and viewing it as a valuable security enhancement. The high satisfaction rate (90%) suggests that biometric measures would be well-received and effective in fostering a secure study environment. Given that 85% of respondents favored fingerprint recognition over other methods such as hand geometry (10%) and voice recognition (5%), fingerprint scanning appears to be the most suitable choice. This preference is likely due to its balance of security, ease of use, and relatively low cost, making it an accessible yet effective option that aligns with user expectations for streamlined and reliable access control in the library setting.

CONCLUSION

In this research work, we discussed on how biometric authentication will benefit the Katsina State Institute of Technology and Management (KSITM) library in the increased of securing their data. And according to the research conducted finger print method was chosen as the system to be used in the Institute Library. However, biometric systems are not entirely foolproof; hackers have developed methods to bypass these systems, revealing that they can still be vulnerable to certain attacks. Despite their advantages, biometrics require ongoing advancements to maintain security against evolving threats.

REFERENCES

Albalawi, S., Alshahrani, L., Albalawi, N., Kilabi, R., & Alhakamy, A. (2022). A Comprehensive Overview on Biometric Authentication Systems using Artificial Intelligence Techniques. *International Journal of Advanced Computer Science and Applications*, *13*(4), 782–791. https://doi.org/10.14569/IJACSA.2022.0130491

Byron, C. D., Kiefer, A. M., Thomas, J., Patel, S., Jenkins, A., Fratino, A. L., & Anderson, T. (2021). The authentication and repatriation of a ceremonial tsantsa to its country of origin (Ecuador). *Heritage Science*, *9*(1), 1–13. https://doi.org/10.1186/s40494-021-00518-z

Israa M. Alsaadi. (2012). Physiological Biometric Authentication Systems, Advantages, Disadvantages and Future Development : A Review. *International Journal of Scientific & Technology Research*, *1*(1).

Kamble, P., Jadhav, H., Raste, D., Bhange, T., & More, S. S. (2024). *International Journal of Research Publication and Reviews Biometric Authentication : Security, Development and Future work*. *5*, 4882–4889.

Majeed Alsaadi, I. (2021). Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: a review. *International Journal of Scientific & Technology Research*, *10*(January), 1. https://www.researchgate.net/publication/348662448

Phadke, S. (2013). The Importance of a Biometric Authentication System. *The SIJ Transactions on Computer Science Engineering & Its Applications (CSEA)*, *01*(04), 18–22. https://doi.org/10.9756/sijcsea/v1i4/0104550402

Pujari, V., Patil, R., & Sutar, S. (2021). Research paper on biometrics security. *Contemporary Research in India*, *June*.

Weaver, A. C. (2006). Biometric authentication. *Computer*, *39*(2), 96–97. https://doi.org/10.1109/MC.2006.47