



A Secured Digital Document Management System using Fingerprint Signature

¹Ghaniyyat Bolanle Balogun, ²Moses Oluwaseyi Akinola, ³Rantiola Fidelis Famutimi, ⁴Fatima Enehezei Usman-Hamza, ⁵Peter Ogirima Sadiku, ⁶Suhurat Ikeola Olatinwo, ⁷Taibat Olaoluwa Adebakin, ⁸Abdulrafii Muhammed Jamiu

^{1,2,4,5,6,7&8}Department of Computer Science, Faculty of Communication and Information Science, University of Ilorin, Ilorin

³Department of Mathematical and Computer Sciences, University of Medical Sciences, Ondo City, Ondo State, Nigeria

ABSTRACT

In today's digital world, the need for secure and efficient document management systems is paramount. The ever-growing reliance on digital documents necessitates robust security measures to protect sensitive information and combat unauthorized access to information. This led to the aim of this research which is to develop a Digital Document Management System (DDMS) that leverages fingerprint signatures for enhanced security and user convenience. The methodology engages the use of cutting-edge software development kits and tools which includes Kotlin, PostgreSQL, and some Java Virtual Machine (JDK) framework. This methodology integrates fingerprint signature together with Digital Document Management System. The key features of the system include document encryption, access control with fingerprint signature, and document storage. The result reveals a highly secured document management system immune to security breaches like brute-force attack and credential impersonation. The Digital Document Management System (DDMS) secure with fingerprint signature can serve as a solution to many documents' security challenges.

ARTICLE INFO

Article History

Received: March, 2026

Received in revised form: March, 2026

Accepted: June, 2026

Published online: June, 2026

KEYWORDS

Digital Document Management System,
Fingerprint Signature, Document Security,
Access Control, Encryption

INTRODUCTION

Despite the numerous benefits of advanced digital document management systems, security vulnerabilities remain a critical concern, particularly in the realm of user authentication. Many organizations still face challenges in implementing an effective and secure system for digital document storage and management. Conventional methods such as passwords and pins can be forgotten, stolen, or leaked, vulnerable to breaches through theft, hacking, or social engineering attacks thereby compromising the integrity of sensitive documents. While digital signatures offer some level of authentication, they can be compromised through forgery or impersonation if unauthorized individuals gain access to the signing credentials. Additionally, the process of manually signing documents can be both time-consuming and

prone to errors. Therefore, there is a pressing need for a more robust, reliable, and secure authentication method that leverages biometric authentication, specifically fingerprint recognition for accessing digital document management systems, to ensure the authenticity and confidentiality of documents (Yusuf et al, 2020).

The purpose of a digital signature is the same as that of encryption key but with a higher level of security, this attributes the signer of the document to the document and registers a binding commitment to the document. While some existing systems already leverage the advantages of using fingerprint recognition for document management systems, there are still challenges that need to be addressed. One of the main issues is the lack of a comprehensive system that integrates fingerprint recognition with document management functionalities. Existing systems either focus

Corresponding author: Ghaniyyat Bolanle Balogun,

balogun.gb@unilorin.edu.ng

Department of Computer Science, Faculty of Communication and Information Science, University of Ilorin, Ilorin, Nigeria.

© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved



solely on fingerprint authentication or document management, but not both. There is a need for a system that efficiently integrate fingerprint authentication into DDMS for a secured document management.

In today's digital age, the need for efficient and secure document management systems is more important than ever. Traditional paper-based document management systems are not only cumbersome and time-consuming but also prone to security breaches. With the advent of computers, centralized computers (servers) and electronic document management systems (EDMS), organizations can now store documents electronically in the centralized computer. Digital Document Management Systems (DDMS) have become indispensable systems in modern organizations and firms as they offer immersive benefits such as reduced cost of document management, streamlined document workflows, and enhanced collaboration and security. This system allows for the storage, retrieval, and management of electronic documents, reducing the need for physical storage space and minimizing the risk of document loss or misplacement.

While DDMS has enhanced security over traditional document management systems, among other challenges like Inefficient Document Workflow, Insufficient Authentication Security, Insufficient Authentication Security, Identity-related Threats, and Compliance and Legal Concerns, one of the key challenges of digital document management systems is ensuring secure and reliable authentication of users and the documents. Standard security measures that rely on passwords and pins can be easily forgotten, stolen, or hacked, leading to potential breaches of confidentiality and unauthorized access to sensitive information. Document security breaches and data leaks pose significant risks to organizations, and there is a need for an advanced security layer.

The concerns about the security of digital documents and the potential for unauthorized access necessitate the exploration of advanced authentication methods. It is essential to provide enhanced authentication

performance to overcome the limitations regarding accuracy, robustness, and vulnerability to spoofing attacks for a secure and reliable authentication system (Vinayagam et al., 2024). One promising solution is the use of biometric authentication, specifically fingerprint signatures (Sudarsono et al, 2017). (Vinayagam et al., 2024) stated that the most efficient way of identifying and authenticating individuals centered on unique biological characteristics, which are distinctive and appropriate only to them, is biometric authentication. Biometric authentication methods have gained popularity for their accuracy and convenience. Fingerprint signatures are unique to each individual and cannot be easily forged, making them a highly secure method of verifying the identity of document signatories.

This study aims to develop a digital document management system that leverages the strength of the cryptography and convenience of biometric authentication (fingerprint signature) to offer enhanced user authentication, protect against identity-related threats, ensure legal validity, streamline document workflows, and establish a comprehensive audit trail for accountability. Fingerprint recognition offers a higher level of security, as each individual's fingerprint is unique and cannot be easily replicated or stolen. In addition to enhanced security, a digital document management system utilizing fingerprint signatures can streamline workflow processes and improve productivity. Users can quickly and easily access documents, track changes, and collaborate with team members in real time, all while ensuring the confidentiality and integrity of sensitive information. Overall, this study seeks to explore the potential benefits of integrating fingerprint signatures into a digital document management system and to demonstrate the feasibility and effectiveness of this technology in enhancing security and efficiency in document management practices.

METHODOLOGY

System Architecture

The Digital Document Management System consists of three main components: the

Corresponding author: Ghaniyyat Bolanle Balogun,

balogun.gb@unilorin.edu.ng

Department of Computer Science, Faculty of Communication and Information Science, University of Ilorin, Ilorin, Nigeria.

© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved

client application (front-end), server (back-end), and database. While the front-end is responsible for user interactions and interfaces, the back-end handles the business logic and data processing, and the database stores that handles all data related to the system.

Architectural Model

1. **Client Application (Front-end):** This component will be used by users to access the system. This component is made up of the following smaller modules:

Biometric Module: Integrated fingerprint scanner for capturing and verifying fingerprints.

User Interface: This module is for interacting with the system after successful security verification. Users will be able to upload, view, and manage their documents through the user-friendly interface. The front-end of the system will be designed using Kotlin for a desktop app. This will involve developing a

user-friendly interface for document management and signature capture.

2. **Server (Back-end):** Central repository for storing documents and managing user data. The back-end will be developed using Kotlin for server-side scripting, which will handle the authentication and authorization process using the secured fingerprint signature technology. This component is made up of the following smaller modules:

Application Programming Interface (API): This is the module that governs the operations of the system. It connects the all other modules together.

Document Store: This is where the users' document is stored.

Fingerprint Database: The proposed fingerprints storage. The database will be implemented using MySQL to store all user and document information securely.

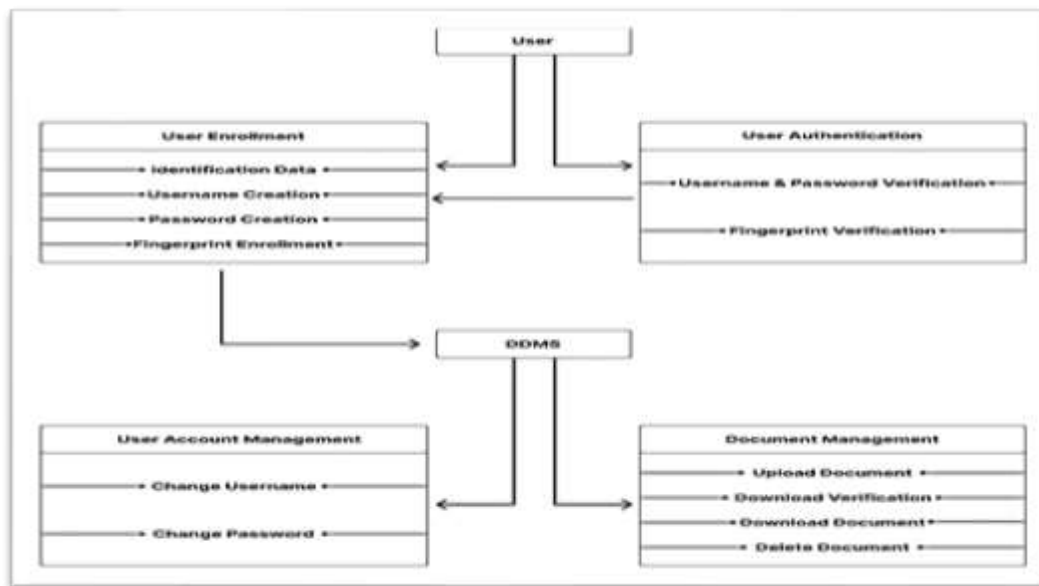


Figure 1: Use Case Diagram

Fingerprint Enrolment

Fingerprint Capture: Captures fingerprints for two fingers from a fingerprint reader.

Quality Check: Checks image quality to ensure that a good quality scan is obtained.

Feature Extraction: Extracts the fingerprint minutiae.

Save: Saves the fingerprint minutiae in a database in text format.

Fingerprint Authentication

Fingerprint Capture: From a fingerprint reader, capture a fingerprint image of either of the two enrolled fingers of the user.

Feature Extraction: Extracts the fingerprint minutiae.

Verification: Compares extracted features with stored templates to authenticate users, ensuring high accuracy and security.

Fingerprint and Password Protection:

Password Protection: The password is encrypted with BCrypt Encryption algorithm.

Fingerprint Protection: Stores fingerprint templates using **AES-256 Encryption algorithm** prevent illegal access.

Secure Storage:

All biometric data is stored in a highly secure database with restricted access, complying with data protection regulations.

Document Management:

Upload and Storage: Users can upload documents, which are then encrypted using

AES-256 encryption and stored in the document store.

Retrieval: Authenticated users can retrieve documents via the desktop user interface.

Data Encryption

Encryption key: Encryption key generation is based on PBKDF2WithHmacSHA256 algorithm. The algorithm requires a password text and a salting text. One of the enrolled fingerprint's text values will be used as the password and the other as the salting text

AES-256

Encryption: Ensures that all documents are encrypted during storage and transmission, providing a high level of security.

SSL/TLS: Secures data transmission between the client and server, preventing unauthorized access during communication.

Data Flow Diagram (DFD)

This is a visual representation of data movement within the proposed system. The DFD provides a visual representation of data movement within the system. It highlights how user inputs (fingerprints and documents) are processed and stored securely.

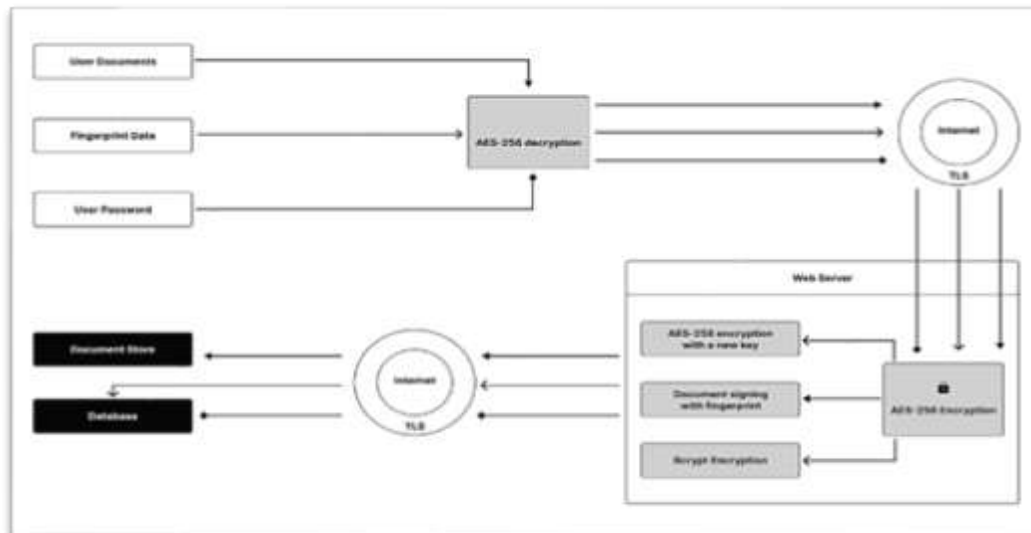


Figure 2: Data Flow Diagram

Corresponding author: Ghaniyyat Bolanle Balogun,

baloqun.gb@unilorin.edu.ng

Department of Computer Science, Faculty of Communication and Information Science, University of Ilorin, Ilorin, Nigeria.

© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved

RESULTS AND DISCUSSION

Graphical User Interface

This shows the outlook (user Interface) of the implementation of the proposed system on a windows desktop device. The user interface consists of pages exhibiting the functionalities or procedures for using the system.

Registration Page Design

The registration page will allow new users to create an account and enrol two of their fingers for fingerprint authentication. The page has the following key elements: User Information, Full Name and Email Address.



The registration form is titled 'Sign In Sign Up'. It contains two sections: 'Tell us your names' with input fields for 'First Name*', 'Middle Name', and 'Last Name*'; and 'Identity Details' with input fields for 'Enter a valid Email*' and 'Select a username'. A 'Continue' button is at the bottom.

Figure 3: User information

Fingerprint Enrolment

A fingerprint scanner will be integrated into the registration page. Users will be guided through the process of scanning and enrolling their fingerprint with the system. This biometric data will be securely stored for future authentication. Once the user information and fingerprint enrolment are complete, the user can submit the registration form to create their account. The system will validate the input data and generate a unique user ID. The registration page will provide a seamless onboarding experience while prioritizing the security of user accounts and biometric data. Upon successful registration, the user will receive a confirmation message and be redirected to the dashboard page.



Figure 4: Fingerprint Enrolment (Step 1)



Figure 5: Fingerprint Enrolment (Step2)

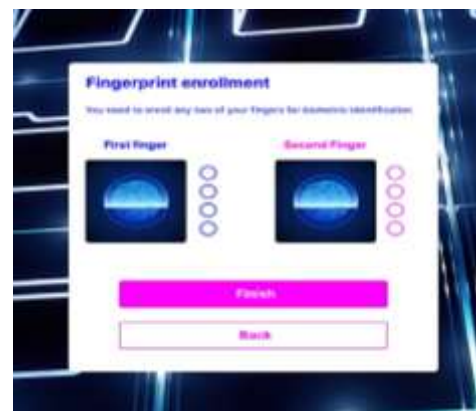


Figure 6: Fingerprint Enrolment (Step 3)

Sign-in Page Design

The sign-in page will allow registered users to securely access the Digital Document Management System. This page consists of the following key elements:

User Authentication: Users will be prompted to enter their login credentials, which consist of: Email Address/Username and Password.

Fingerprint Authentication: In addition to the traditional username and password, users will have to authenticate using either of their registered fingerprints. This biometric login method will provide an extra layer of security and convenience.

Error Handling: The sign-in page will provide clear and helpful error messages if the user enters invalid credentials or encounters any other issues during the authentication process. This will help users troubleshoot and sign in successfully. Upon successful authentication, the user will be redirected to the main dashboard of the system, where they can access the full range of document management features.



Figure 7: Sign in Page



Figure 8: Sign in Fingerprint Authentication

Dashboard Page: The dashboard page serves as the central hub for users to interact with the system. It provides an overview of the user's activities and access to the core features. The dashboard includes the following key elements:

Welcome Message: The dashboard greets the user with a personalized welcome message that shows their name.

Document Overview: The dashboard displays key information about documents own by the user. Information displayed includes: document name, upload date and document format.

Quick Actions: The dashboard provides quick access to the most common user actions, including uploading a new document, accessing the document repository and managing user profile and settings.

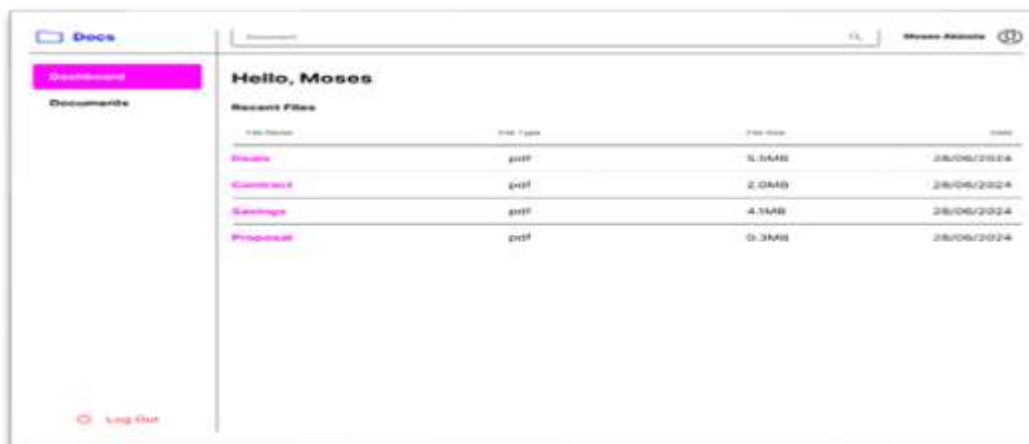


Figure 9: Dashboard Page

Corresponding author: Ghaniyyat Bolanle Balogun,

balogun.gb@unilorin.edu.ng

Department of Computer Science, Faculty of Communication and Information Science, University of Ilorin, Ilorin, Nigeria.

© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved



Testing

This phase involves systematic evaluation of the software to detect defects, ensure quality, and verify that software meets the specified requirements and objectives. This testing is essential to ensure that the system is reliable, user-friendly, secure, and performs well under various conditions. Given the critical nature of the Digital Document Management System and the sensitive data it handles, thorough software testing is essential to ensure the system's reliability, security, and compliance. The objective is to ensure that the DDMS meets the defined requirements and operates effectively in real-world scenarios.

System security

System security in the Digital Document Management System with Secured Fingerprint Signature is paramount to safeguarding sensitive documents and user information. The integration of fingerprint authentication in the system adds a security layer that to give the system a robust security posture to safeguard sensitive documents. By implementing robust security measures, conducting regular assessments, and adhering to compliance standards, the DDMS ensures data confidentiality, integrity, and availability, thereby building trust and reliability among users and stakeholders.

CONCLUSION

The successful development and implementation of the Digital Document Management System Using Secured Fingerprint Signature has resulted in a comprehensive, secure, and user-friendly solution for document management. This research addresses the growing need for efficient digital document management while incorporating innovative biometric security measures to protect sensitive information. The developed system addresses the limitations of traditional paper-based systems and the existing digital solutions with weak security measures. By leveraging fingerprint authentication for user access control, document signing, and potential verification processes, the research offers a robust and user-friendly solution.

Through a thorough review of the existing literature, the research team identified key gaps in the security of digital document management. The integration of fingerprint biometrics for user authentication has added a robust layer to protection in document management. This is achieved by ensuring that only authorized personnel can access and manage the digital documents.

By leveraging the strengths of PostgreSQL as the underlying database and adhering to industry best practices, the system was designed and implemented with a focus on data integrity, security, scalability, and extensibility. The seamless incorporation of this feature into the document management workflows has provided a convenient and secure user experience, addressing the growing concerns around data privacy and compliance. The comprehensive testing strategy, including unit testing, integration testing, and usability evaluation, has helped ensure the reliability, functionality, and user-friendliness of the Digital Document Management System.

Acknowledgements

There is no grant or funding bodies to be acknowledged for preparing this paper.

REFERENCES

- Almacen, A.M., & Cabaluna, A.Y. (2021). Electronic Document Management System (EDMS) Implementation: Implications for the Future of Digital Transformation in Philippine Healthcare. *Journal of Computer Science and Technology Studies*.
<https://doi.org/10.32996/jcsts.2021.3.2.8>
- Balogun, N.A., Raheem, L.A., Abdulrahman, M.D., & Balogun, U.O. (2019). Adoptability of electronic document management system in Ilorin businesses. *Nigerian Journal of Technology*, 38, 707-715.
[10.4314/njt.v38i3.24](https://doi.org/10.4314/njt.v38i3.24)
- Bedari, A., Wang, S., & Yang, W. (2022). A secure online fingerprint authentication system for industrial iot devices over 5g networks. *Sensors*, 22(19), 7609.
<https://doi.org/10.3390/s22197609>
- Das, A., Galdi, C., Han, H., Ramachandra, R., Dugelay, J. L., & Dantcheva, A. (2018).

Corresponding author: Ghaniyyat Bolanle Balogun,

balogun.gb@unilorin.edu.ng

Department of Computer Science, Faculty of Communication and Information Science, University of Ilorin, Ilorin, Nigeria.

© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved



- Recent Advances in Biometric Technology for Mobile Devices. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 1-11.
- Islam, M. A., Sarder, M. S., Mamun, M. H., Ahmed, F., Sarkar, S. K., Mridul, A. H., ... & Khatun, T. (2022). *Multi Level Bank Locker Security System with Digital Signature Authentication and Internet of Things*. <https://doi.org/10.21203/rs.3.rs-2173423/v1>
- Leghari, M., Memon, S., Dhomeja, L. D., Jalbani, A. H., & Chandio, A. A. (2021). Deep feature fusion of fingerprint and online signature for multimodal biometrics. *Computers*, 10(2), 21. <https://doi.org/10.3390/computers10020021>
- Muminova, s., erkinovna, q.k., sobirovna, t.s., & abduamatovich, i.a. (2024). Developing an electronic document management solution tailored for local area network (lan) dependent organizations. *International Journal of Advance Scientific Research*.
- Mustapää, T., Tunkari, H., Taponen, J., Immonen, L., Heeren, W., Baer, O., ... & Viitala, R. (2022). Secure Exchange of Digital Metrological Data in a Smart Overhead Crane. *Sensors*, 22(4), 1548. <https://doi.org/10.3390/s22041548>
- Pagayonan, S. M. S. (2021). Record Management System with Document Control. *International Journal of Multidisciplinary Research and Analysis*, 4(12), 1929-1934.
- Rahmawati, E., Listiyasari, M., Aziz, A.S., Sukaridhoto, S., Damastuti, F.A., Bachtar, M.M., & Sudarsono, A. (2017). Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone. In *2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)*, 234-238. 10.1109/ELECSYM.2017.8240409.
- Saxena, S., & Anand, D. (2017). A novel digital signature algorithm based on biometric hash. *International Journal of Computer Network and Information Security*, 9(1), 12.
- Shahid, F., & Khan, A. (2020). Smart Digital Signatures (SDS): A post-quantum digital signature scheme for distributed ledgers. *Future Generation Computer Systems*, 111, 241-253. <https://doi.org/10.1016/j.future.2020.04.042>
- Shankar, G., Ai-Farhani, L. H., Anitha Christy Angelin, P., Singh, P., Alqahtani, A., Singh, A., ... & Samori, I. A. (2023). Improved multisignature scheme for authenticity of digital document in digital forensics using edward-curve digital signature algorithm. *Security and Communication Networks*, 2023(1), 2093407. <https://doi.org/10.1155/2023/2093407>
- Kim, T., Oh, Y., & Kim, H. (2020). Efficient Privacy-Preserving Fingerprint-Based Authentication System Using Fully Homomorphic Encryption. *Security and Communication Networks*, 2020(1), 4195852. <https://doi.org/10.1155/2020/4195852>
- Thakur, A., Singh, R., & Choi, Y. (2017). A review paper on digital signature authentication techniques. *International Journal of Advanced Research in Computer Science*, 8(5), 690-694.
- Therar, H. M., & Ali, A. J. (2022). Personal authentication system based on iris recognition and digital signature technology. *Journal of Soft Computing and Data Mining*, 3(1), 1-18.
- Tseng, K. K., Chen, H., Chen, C., & Bansong, C. (2021). A secure live signature verification with Aho-Corasick histogram algorithm for mobile smart pad. *Electronics*, 10(11), 1337. <https://doi.org/10.3390/electronics10111337>
- Yudistira, R. (2024). AES (Advanced Encryption Standard) and RSA (Rivest Shamir Adleman) Encryption on Digital Signature Document: A Literature Review: Watermarking, Digital Signature, AES, RSA, Literature Review. *International Journal of Information Technology and Business*, 7(1), 29-31. <https://doi.org/10.24246/ijiteb.712022.29-31>
- Yusuf, N., Marafa, K.A., Shehu, K.L., Mamman, H., & Maidawa, M. (2020). A survey of biometric approaches of authentication. *International Journal of Advanced Computer Research*, 10(47), 96-104. <http://dx.doi.org/10.19101/IJACR.2019.940152>

Corresponding author: Ghaniyyat Bolanle Balogun,

balogun.gb@unilorin.edu.ng

Department of Computer Science, Faculty of Communication and Information Science, University of Ilorin, Ilorin, Nigeria.

© 2026. Faculty of Technology Education. ATBU Bauchi. All rights reserved