AI-Based Digital Document Authenticity Verifier: Enhancing Document Security at Jesus Reigns Christian College

Aliah Turla Evangelista[1], John Michael Garra Amad[2], Diana Joss Conda Sualog[3], Vivien Accad Agustin[4], Ronald Burdios Fernandez[5]

[1'2'3]Department of Information Technology, Jesus Reigns Christian College, Malate Manila, Philippines

[4'5]La Consolacion University, Philippines

DOI: https://doi.org/10.51244/IJRSI.2026.1305000276

Received: 18 May 2026; Accepted: 23 May 2026; Published: 15 June 2026

ABSTRACT

The increasing use of digital academic documents has raised concerns regarding document tampering, forgery, and the inefficiency of manual verification processes in educational institutions. Traditional methods of verifying academic records are often time-consuming, prone to human error, and vulnerable to unauthorized modifications. In response to these issues, this study entitled "AI-Based Digital Document Authenticity Verifier: Enhancing Document Security at Jesus Reigns Christian College" aimed to develop a secure, efficient, and automated system capable of verifying the authenticity of digital academic documents.

The study utilized a developmental research design and followed the Waterfall Model under the Software Development Life Cycle (SDLC). The proposed system integrates Artificial Intelligence (AI), Secure Hash Algorithm (SHA-256), blockchain verification logging, and a Document Management System (DMS) to improve document security and verification accuracy. The AI component analyzes document content, formatting, metadata, and structure to detect possible signs of tampering, while the SHA-256 algorithm generates unique hash values to ensure document integrity. The system also includes features such as real-time tampering alerts, cloud backup, verification reports, and organized document storage to improve usability and accessibility.

The development process involved requirements analysis, system design, implementation, integration and testing, deployment, and maintenance to ensure that the system functions effectively and meets institutional requirements. The findings of the study showed that the integration of AI and cryptographic hashing significantly enhances the reliability, speed, and accuracy of document verification compared to traditional manual methods. The developed system provides a practical and secure solution for managing and verifying academic documents while minimizing verification errors and strengthening institutional document security at Jesus Reigns Christian College.

Keywords: Artificial Intelligence (AI), Digital Document Verification, SHA-256, Blockchain Technology, Document Management System (DMS), Academic Document Security, Tampering Detection, Automated Verification.

INTRODUCTION

The continuous advancement of digital technology has greatly influenced the way educational institutions manage and process academic records and official documents. Many schools and universities now rely on digital platforms for handling certificates, transcripts, permits, and other important records because of their convenience, accessibility, and efficiency. Despite these advantages, the increasing use of digital documents has also created concerns regarding document forgery, unauthorized modification, and data security. Manual verification methods are often slow, labor-intensive, and dependent on human observation, making them vulnerable to errors and ineffective in identifying sophisticated forms of document tampering.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

To address these issues, modern technologies such as Artificial Intelligence (AI), blockchain technology, cryptographic hashing, and Document Management Systems (DMS) have been introduced to improve document authentication and security. Artificial Intelligence has the capability to analyze document content, formatting, metadata, and structural patterns to detect irregularities that may indicate tampering. Meanwhile, cryptographic hashing algorithms such as SHA-256 provide a reliable method for preserving document integrity by generating unique digital fingerprints for every file. Blockchain technology further strengthens security by maintaining tamper-proof verification records, while Document Management Systems help organize and securely store verified documents.

Jesus Reigns Christian College handles various academic documents that require accurate verification and secure management. Without an efficient verification system, the institution may encounter challenges related to document authenticity, delays in verification procedures, and risks associated with altered or falsified records. These concerns highlight the importance of implementing a reliable and automated system that can strengthen document security and improve verification processes within the institution.

In response to these concerns, the researchers proposed the development of an AI-Based Digital Document Authenticity Verifier designed to enhance document security and improve the efficiency of document verification. The proposed system integrates Artificial Intelligence for tampering detection, SHA-256 hashing for integrity verification, blockchain-based logging for secure record keeping, and a Document Management System for organized storage and retrieval of files. The system is also equipped with features such as drag-and-drop verification, color-coded trust indicators, real-time alerts, cloud backup, and downloadable verification reports to improve accessibility and usability for users.

Through the implementation of this study, the researchers aim to provide Jesus Reigns Christian College with a secure, efficient, and reliable solution for verifying digital academic documents. The system is expected to minimize manual intervention, reduce verification errors, strengthen document integrity, and improve the overall management of institutional records. Furthermore, the study contributes to the growing development of technology-based document verification systems that support secure and trustworthy academic record management in educational institutions.

METHODOLOGY

This chapter presents the research methodology utilized in the development of the AI-Based Digital Document Authenticity Verifier. It discusses the research design, system development framework, methods, procedures, and tools used to ensure that the proposed system meets the objectives of providing secure, efficient, and reliable document verification for educational institutions. The methodology followed a structured approach to ensure the proper development, implementation, and evaluation of the system.

Research Design

The study employed a developmental research design. This type of research is commonly used in the development or improvement of systems, applications, and technological solutions intended to address real-world problems. The researchers selected this design because the study focused on designing, developing, and evaluating an AI-Based Digital Document Authenticity Verifier intended to enhance document security and improve the verification process within Jesus Reigns Christian College.

The proposed system integrates Artificial Intelligence (AI), Secure Hash Algorithm (SHA-256), blockchain verification logging, and a Document Management System (DMS) to detect document tampering, ensure data integrity, and automate the verification process. Sample academic documents such as certificates, permits, and transcripts were utilized during system testing and evaluation to assess the effectiveness of the verification process.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

System Architecture

The system architecture of the AI-Based Digital Document Authenticity Verifier illustrates how the different components of the proposed system work together to provide secure and efficient document verification. The system integrates Artificial Intelligence (AI), Secure Hash Algorithm (SHA-256), blockchain verification logging, cloud backup, and a Document Management System (DMS) to ensure document authenticity, integrity, and security.

The verification process begins when a user uploads a digital document through the drag-and-drop interface. The AI module then analyzes the document's content, formatting, metadata, and structure to detect possible signs of tampering or inconsistencies. Simultaneously, the SHA-256 hashing mechanism generates a unique hash value that serves as the document's digital fingerprint, allowing the system to identify any unauthorized modifications made to the file.

After verification, the system displays a color-coded trust level and generates real-time tampering alerts whenever suspicious activities are detected. All verification records, reports, and uploaded documents are securely stored in the Document Management System and blockchain verification log for organized management and secure retrieval. Cloud backup is also integrated to ensure data protection and accessibility. Overall, the system architecture provides a reliable, automated, and secure solution for verifying academic documents within Jesus Reigns Christian College.

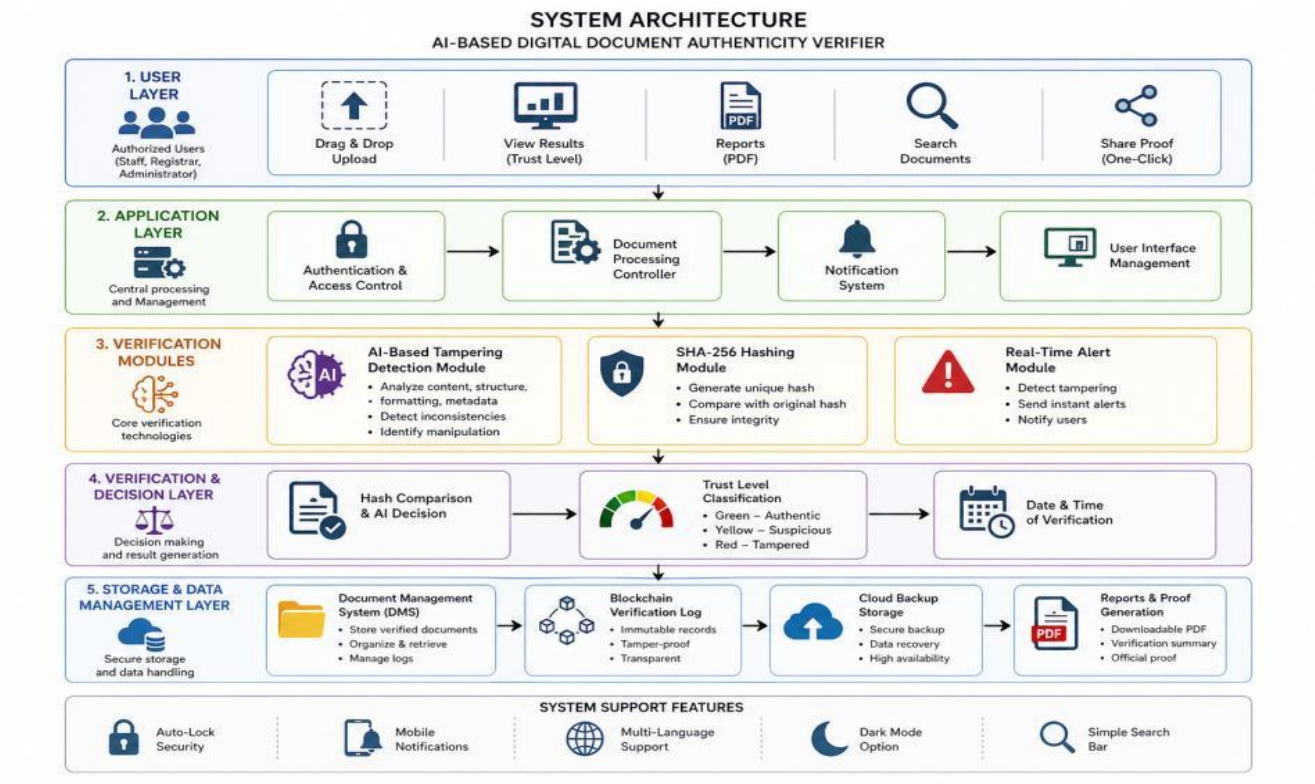

Figure 1. System Architecture

METHODS AND TOOLS

System Methods

Method 1: Waterfall Model (SDLC)

The study utilized the Waterfall Model under the Software Development Life Cycle (SDLC) as the framework for system development. This method follows a sequential process including requirements analysis, system design, implementation, testing, deployment, and maintenance to ensure organized and systematic development.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

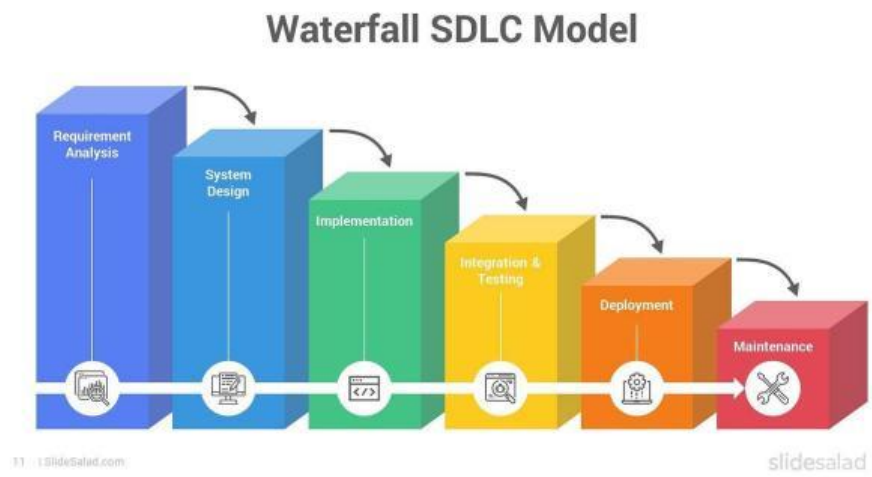

Figure 2. SDLC

Requirements Analysis

The requirements analysis phase is the first stage of the Waterfall Model. During this phase, the researchers identified the problems and limitations of manual document verification within educational institutions. Information was gathered through observations and consultations with potential users such as school administrators and staff. The researchers identified the functional and non-functional requirements needed for the development of the AI-Based Digital Document Authenticity Verifier, including automated verification, tampering detection, security, and usability.

System Design

The system design phase focused on creating the overall structure and framework of the proposed system. In this stage, the researchers designed the system architecture, database structure, workflows, and user interface. The integration of Artificial Intelligence (AI), SHA-256 hashing, blockchain logging, and the Document Management System (DMS) was carefully planned to ensure secure and efficient document verification.

Implementation

The implementation phase involved the actual coding and development of the system based on the finalized design. During this phase, the researchers developed the different components of the system, including the AI module for tampering detection, SHA-256 hashing for integrity verification, and the DMS for document storage and management. The user interface was also created to allow users to upload and verify documents easily.

Integration and Testing

The integration and testing phase involved combining all developed system components and evaluating their functionality, accuracy, and performance. Different testing procedures were conducted to ensure that the system operates properly and can accurately detect tampered documents. Both authentic and manipulated documents were used to assess the reliability and effectiveness of the verification process.

Deployment

The deployment phase involved introducing the completed system into a controlled environment where selected users could access and utilize the platform. During this phase, the researchers monitored the system's performance and ensured that all functionalities operated correctly in real-world conditions. Feedback from users was also gathered to identify possible improvements.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Maintenance

The maintenance phase is the final stage of the Waterfall Model. This phase focuses on monitoring, updating, and improving the system after deployment. The researchers ensured that bugs and errors were fixed, system features were enhanced, and the AI component was continuously improved to maintain system security, reliability, and efficiency over time.

Method 2: AI-Based Document Analysis

The figure presents the AI-Based Document Analysis process integrated into the proposed system through Gemini AI. This method focuses on analyzing uploaded digital documents to identify possible signs of tampering, forgery, or inconsistencies. The AI module examines different components of the document, including its content, formatting, metadata, font consistency, spacing, alignment, and structural patterns. By analyzing these elements, the system can detect anomalies that may not be visible during manual inspection.

Unlike traditional verification methods that rely heavily on human observation, AI-based analysis provides a faster, more objective, and more accurate approach to document authentication. The AI system is capable of identifying both obvious and subtle modifications, such as altered text, inconsistent formatting, manipulated timestamps, and unusual metadata patterns. In addition, the AI component continuously improves its detection capability by learning patterns from authentic and manipulated documents. This method significantly enhances the efficiency, reliability, and accuracy of the verification process while reducing human intervention and verification errors.

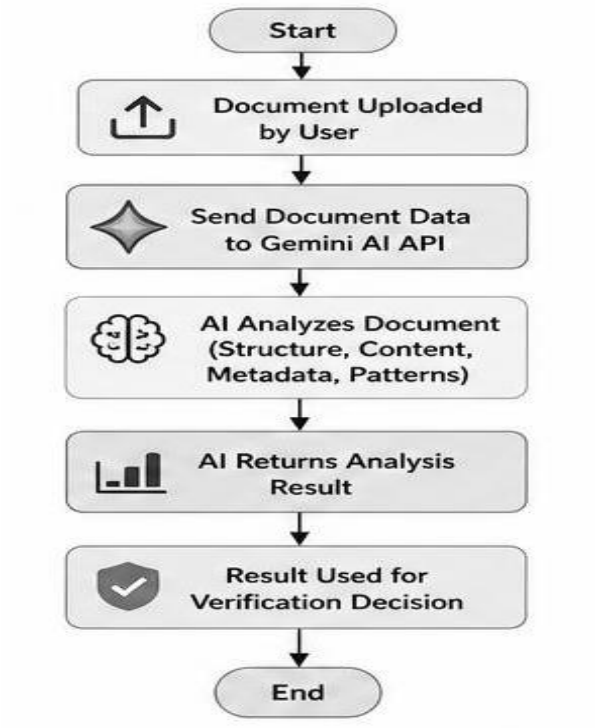

Figure 3. Document Analysis

Method 3: Cryptographic Hashing

The figure illustrates the implementation of the Secure Hash Algorithm (SHA-256) used in the proposed system to ensure document integrity and authenticity. This cryptographic hashing method generates a unique and fixed-length hash value for every uploaded document. The generated hash value serves as the document's digital fingerprint and represents the original content of the file.

One of the important characteristics of SHA-256 is its sensitivity to changes in data. Even the smallest modification made to a document, such as changing a single character or symbol, results in a completely different

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

hash value. The system compares the generated hash value with the stored or expected hash value to determine whether the document has been altered. If the values match, the document is considered authentic; otherwise, the system identifies it as tampered or modified. This method provides a strong layer of security by preventing unauthorized modifications and ensuring that verified documents remain unchanged. Through SHA-256 hashing, the system achieves a secure, reliable, and tamper-resistant verification mechanism.

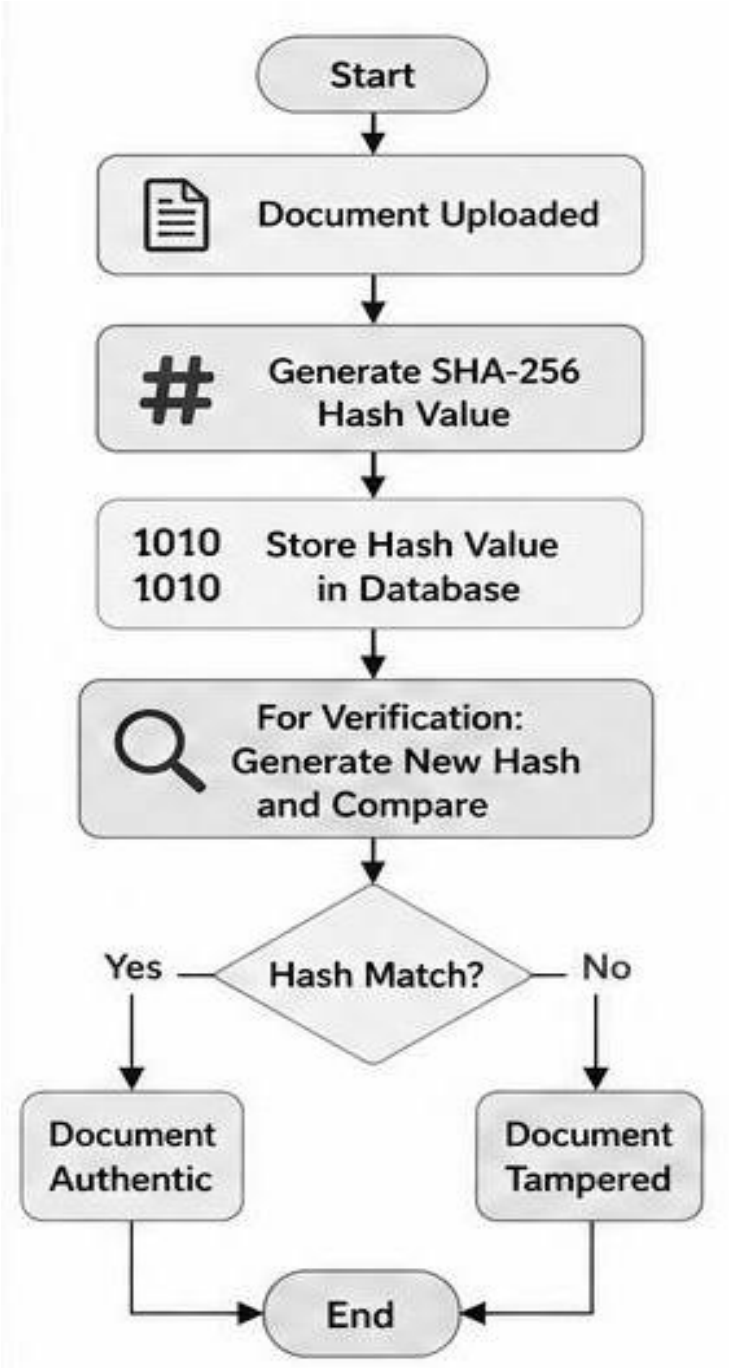

Figure 4. SHA-256

Method 4: Document Management Method

The figure presents the integration of the Document Management System (DMS) within the AI-Based Digital Document Authenticity Verifier. This method is responsible for organizing, storing, managing, and retrieving verified documents and verification records within the system. After the verification process is completed, documents together with their verification results, timestamps, and generated hash values are securely stored in the database.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

The Document Management System categorizes and indexes records to allow users to easily search, retrieve, and manage files using keywords or document identifiers. In addition, the system integrates blockchain logging and cloud backup to further enhance data security and accessibility. Blockchain technology ensures that verification records remain immutable and tamper-proof, while cloud backup protects data from loss and allows remote access across different devices and locations. This method improves efficiency in handling large volumes of documents, reduces redundancy, and ensures that all verification records are securely managed and easily accessible when needed.

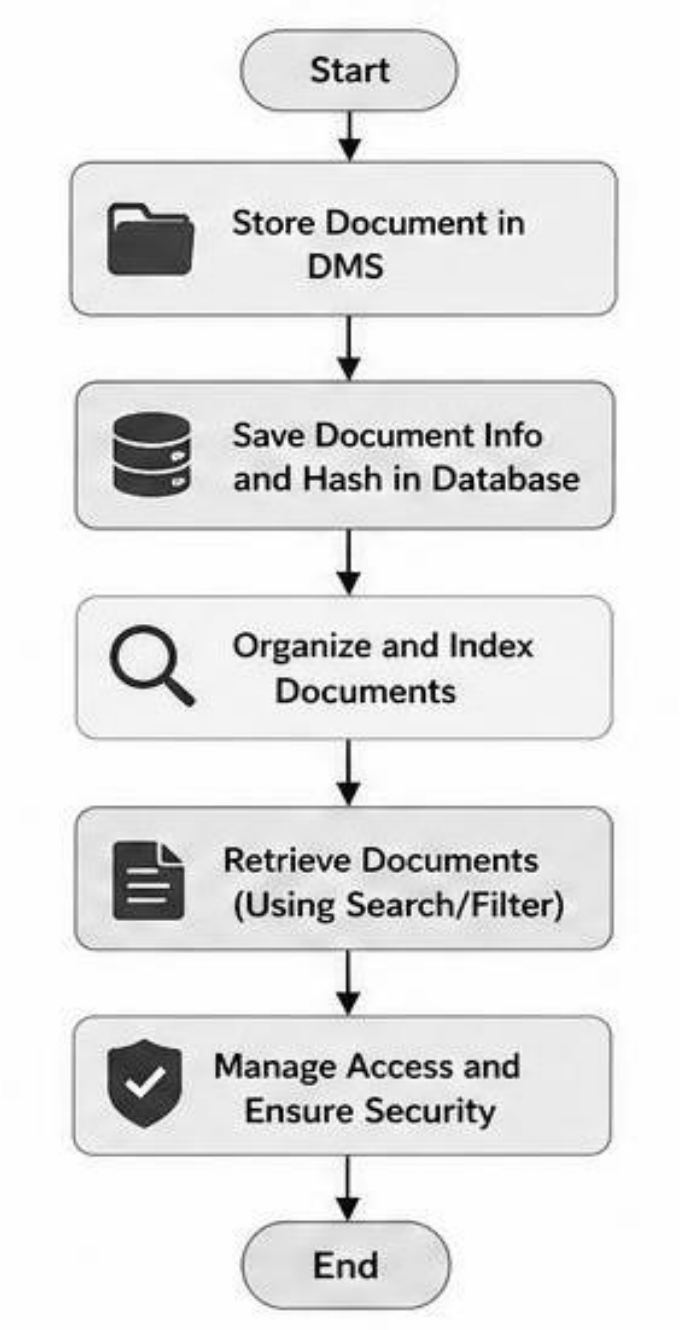

Figure 5. DMS Integration

Method 5: Automated Verification Process

The figure illustrates the automated verification workflow of the proposed system. This method integrates all system components into a unified and automated process that minimizes manual intervention during document verification. The process begins when the user uploads a document through the drag-and-drop interface. The system then performs preprocessing to prepare the uploaded file for analysis and verification.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

After preprocessing, the AI module analyzes the document for inconsistencies and signs of tampering, while the SHA-256 algorithm generates a hash value to verify document integrity. The system combines the results from the AI analysis and cryptographic hashing to evaluate the authenticity of the uploaded document. Once the verification is completed, the system assigns a color-coded trust level indicating whether the document is authentic, suspicious, or tampered. A verification report is then generated, and the results are stored in the Document Management System. Notifications and real-time alerts are also sent to users whenever irregularities are detected. This automated method significantly reduces processing time, improves verification accuracy, minimizes human errors, and ensures consistent and reliable verification results.

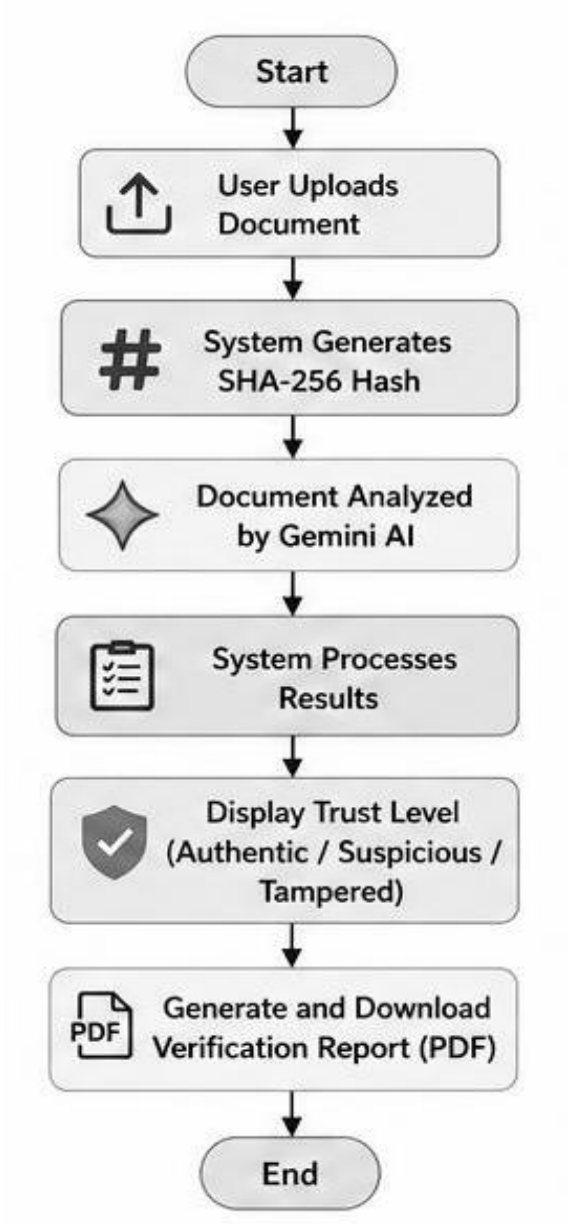

Figure 6. Automated Verification Process

System Tools

Tool 1: PHP

The figure illustrates PHP as the primary backend programming language used in the development of the AI-Based Digital Document Authenticity Verifier. PHP is responsible for handling server-side operations such as processing user inputs, managing document uploads, executing verification procedures, and connecting the system components. It serves as the core technology that links the user interface with the backend processes of the system.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Additionally, PHP enables the integration of Artificial Intelligence, SHA-256 hashing, and the Document Management System within a single platform. It processes requests in real time and ensures smooth communication between the database and the verification modules. Its flexibility, compatibility, and efficiency make it suitable for developing a secure and scalable web-based document verification system.

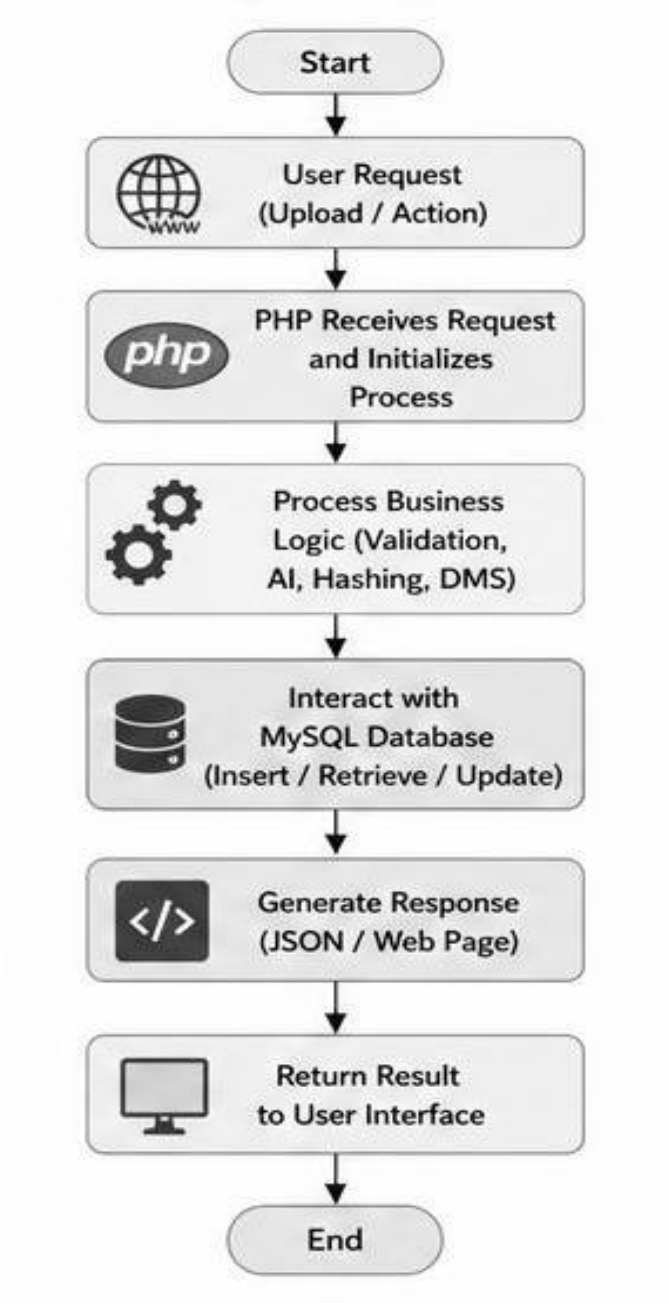

Figure 7. PHP

Tool 2: MySQL

The figure presents MySQL as the database management system utilized in the proposed system. MySQL is responsible for storing and organizing uploaded documents, generated hash values, verification records, timestamps, and user activity logs. It provides a structured and efficient method of handling large amounts of data through relational tables and database queries.

Furthermore, MySQL ensures data consistency, integrity, and security by allowing proper indexing and controlled access to records. It enables the system to retrieve verification histories quickly and maintain an organized repository of digital documents. This tool is important in ensuring reliable record management and efficient document retrieval within the institution.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

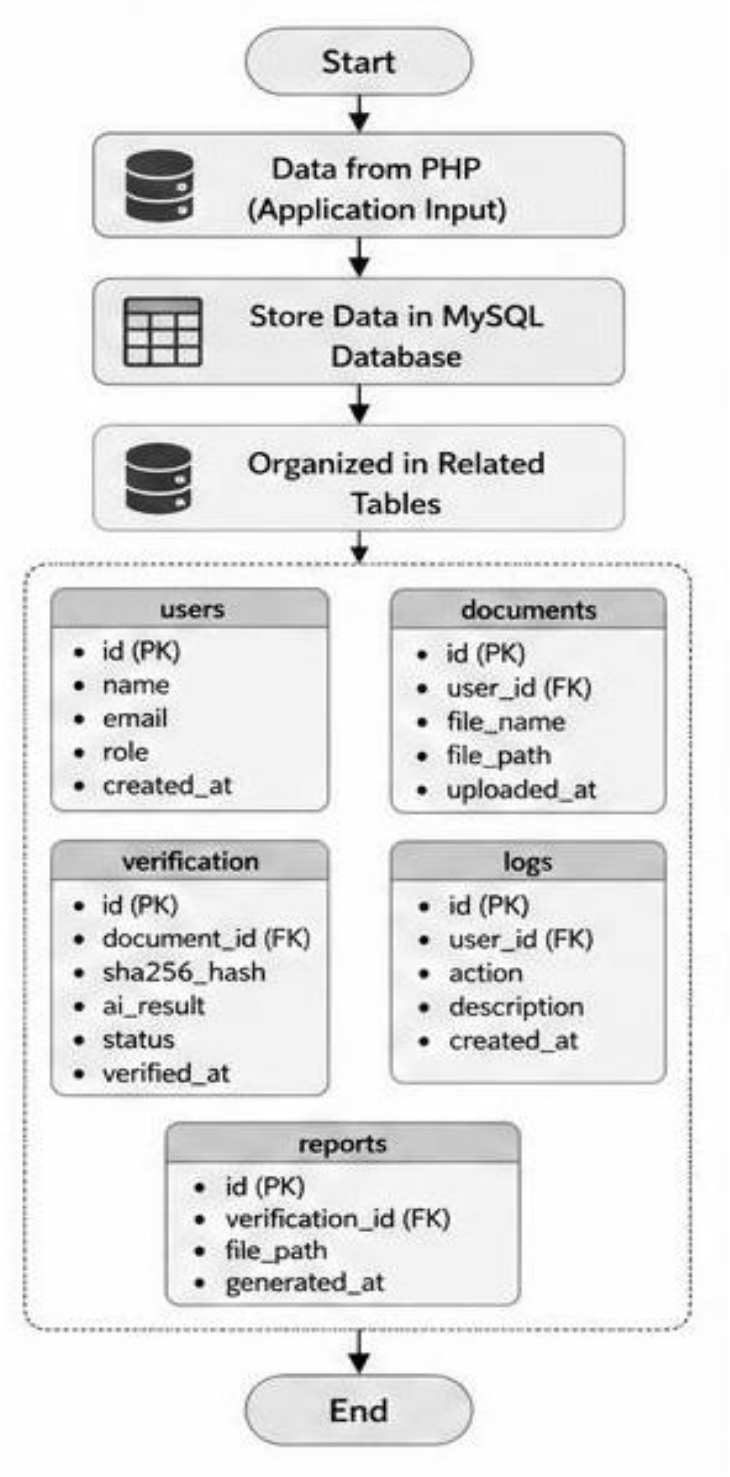

Figure 8. MySQL

Tool 3: Gemini AI API

The figure illustrates the integration of the Gemini AI API within the proposed system. This tool provides advanced Artificial Intelligence capabilities used for analyzing uploaded digital documents. The AI API examines the document's content, formatting, metadata, and structural consistency to identify anomalies or possible signs of tampering.

The Gemini AI API improves the accuracy and reliability of document verification by detecting inconsistencies such as altered timestamps, irregular formatting, unusual spacing, and mismatched font styles. Through AI-based analysis, the system becomes more intelligent, adaptive, and efficient in identifying both obvious and subtle forms of document manipulation.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

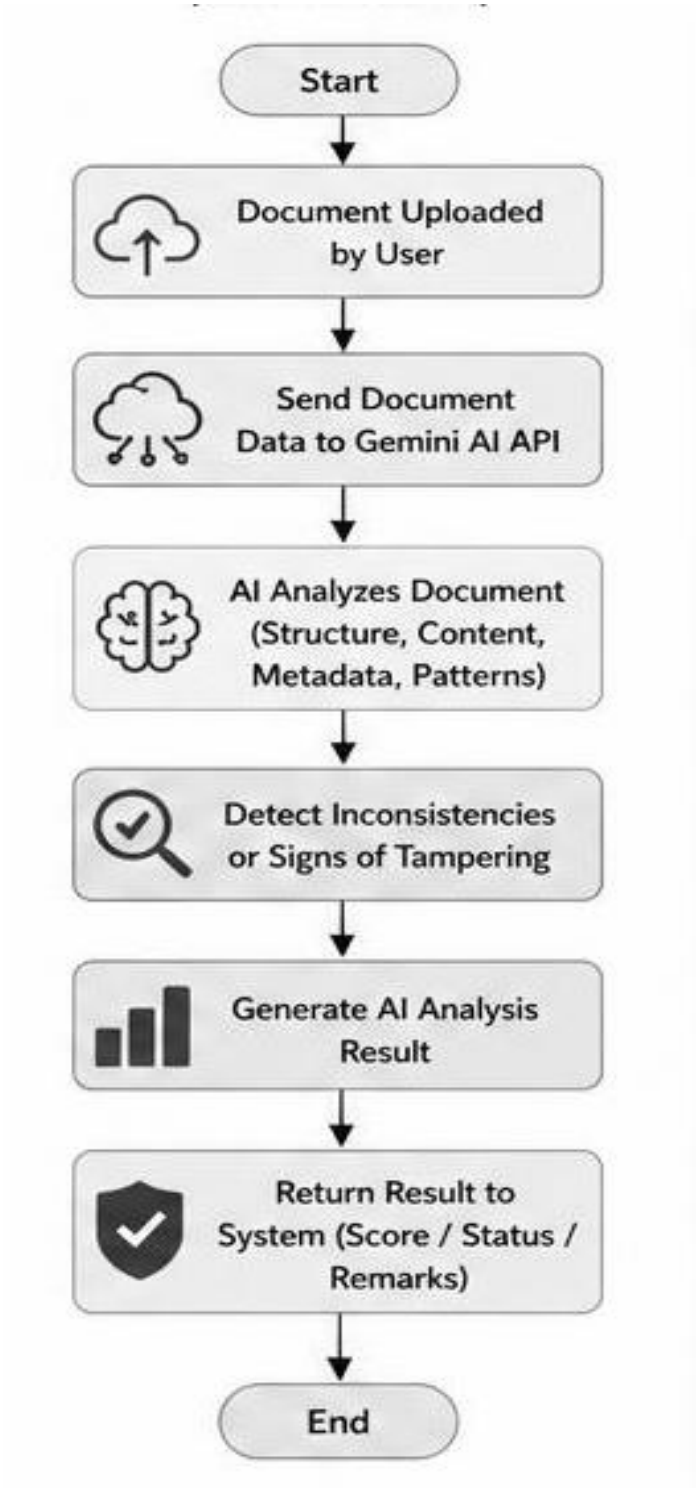

Figure 9. Gemini AI API

Tool 4: Secure Hash Algorithm (SHA-256)

The figure presents the Secure Hash Algorithm (SHA-256) implemented as the cryptographic security mechanism of the system. This tool generates a unique and fixed-length hash value for every uploaded document, which serves as the document's digital fingerprint.

One of the key features of SHA-256 is its ability to detect even the smallest modification made to a file. Any alteration in the document automatically produces a different hash value, allowing the system to identify unauthorized changes quickly and accurately. Through this mechanism, the system ensures document integrity, security, and protection against tampering or forgery.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

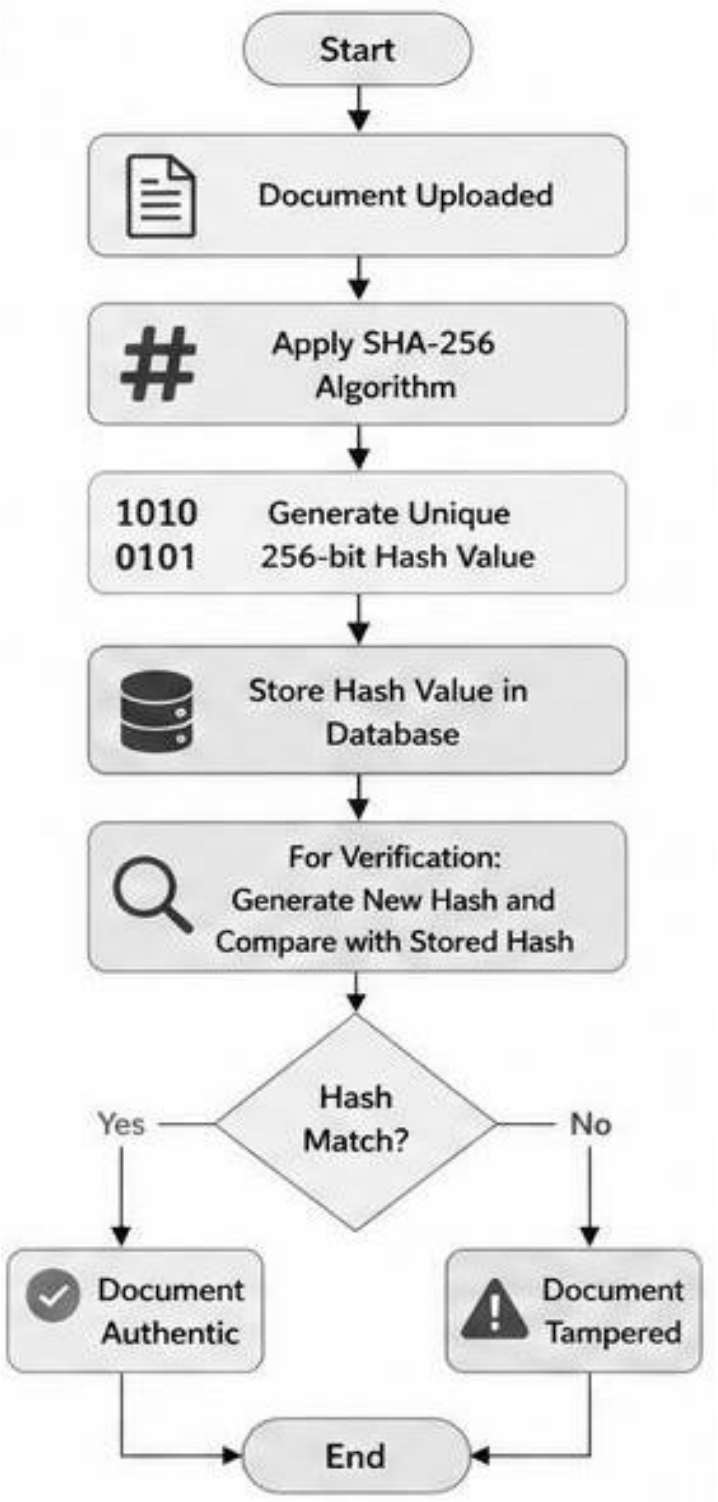

Figure 10. SHA-256

Tool 5: PDF Generator

The figure illustrates the use of FPDF as the PDF generator tool integrated into the system. This tool is responsible for generating verification reports in PDF format after the document verification process is completed. The generated reports include important information such as the document name, verification status, hash value, and verification date.

The PDF generator provides users with downloadable and printable reports that serve as official proof of document authenticity. Using PDF format also ensures compatibility across different devices and platforms, making document sharing and storage more convenient and reliable.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

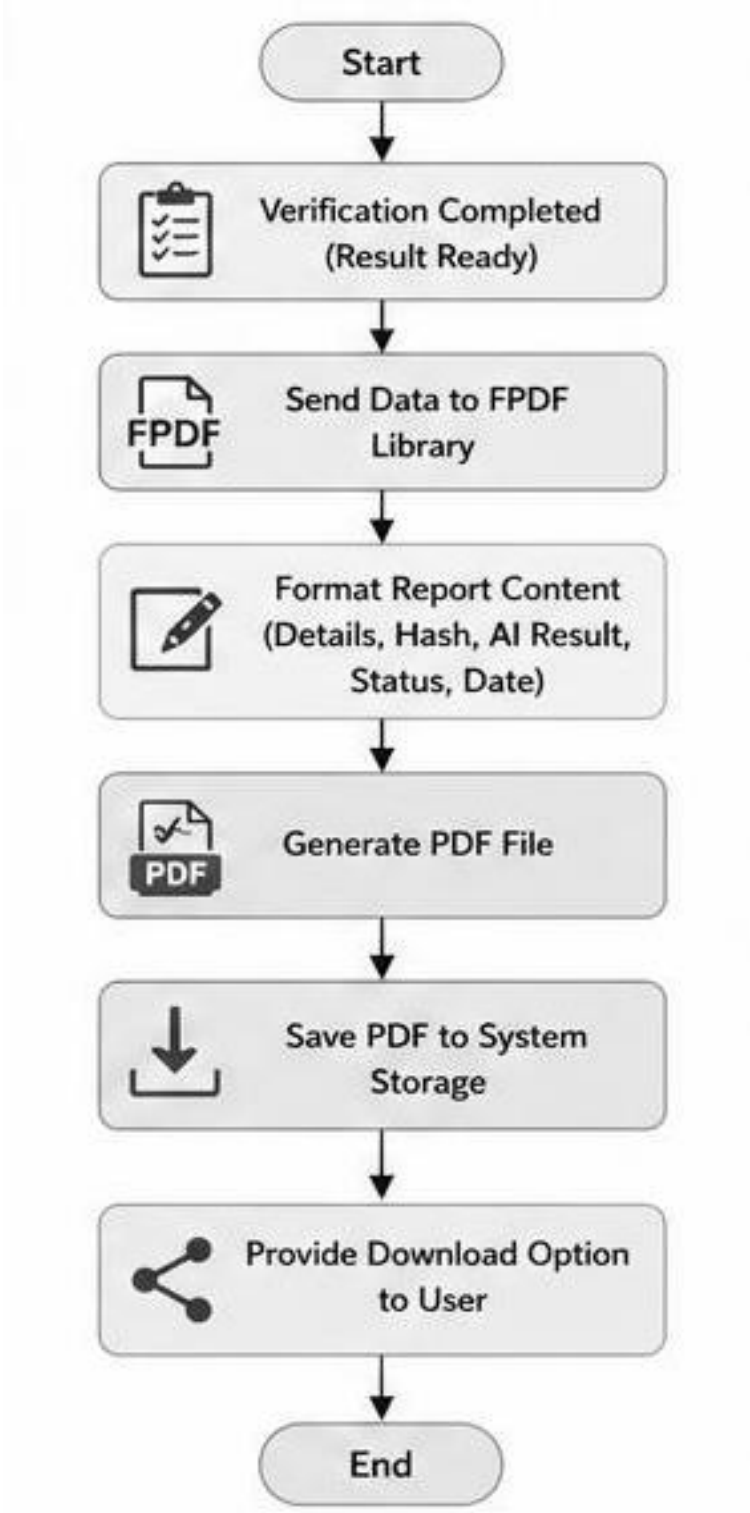

Figure 11. PDF Generator

Tool 6: Local Server Environment

The figure presents XAMPP/WAMP as the local server environment used during the development and testing of the proposed system. This tool provides an environment that includes an Apache web server, PHP interpreter, and MySQL database, allowing the system to run locally without requiring internet-based hosting services.

XAMPP/WAMP helped the researchers perform system development, debugging, testing, and evaluation in a controlled environment. It also ensured smooth integration between PHP and MySQL while allowing the researchers to monitor and improve the performance of the system before deployment.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Figure 12. XAMPP/WAMP

RESULTS AND DISCUSSION

This chapter presents the results gathered from the development and implementation of the AI-Based Digital Document Authenticity Verifier. It discusses the system's features, functionalities, and performance in verifying digital academic documents.

This chapter also explains how the integration of Artificial Intelligence (AI), SHA-256 hashing, and Document Management System (DMS) improved document security, integrity, and verification efficiency at Jesus Reigns Christian College.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

System Administrator Phase

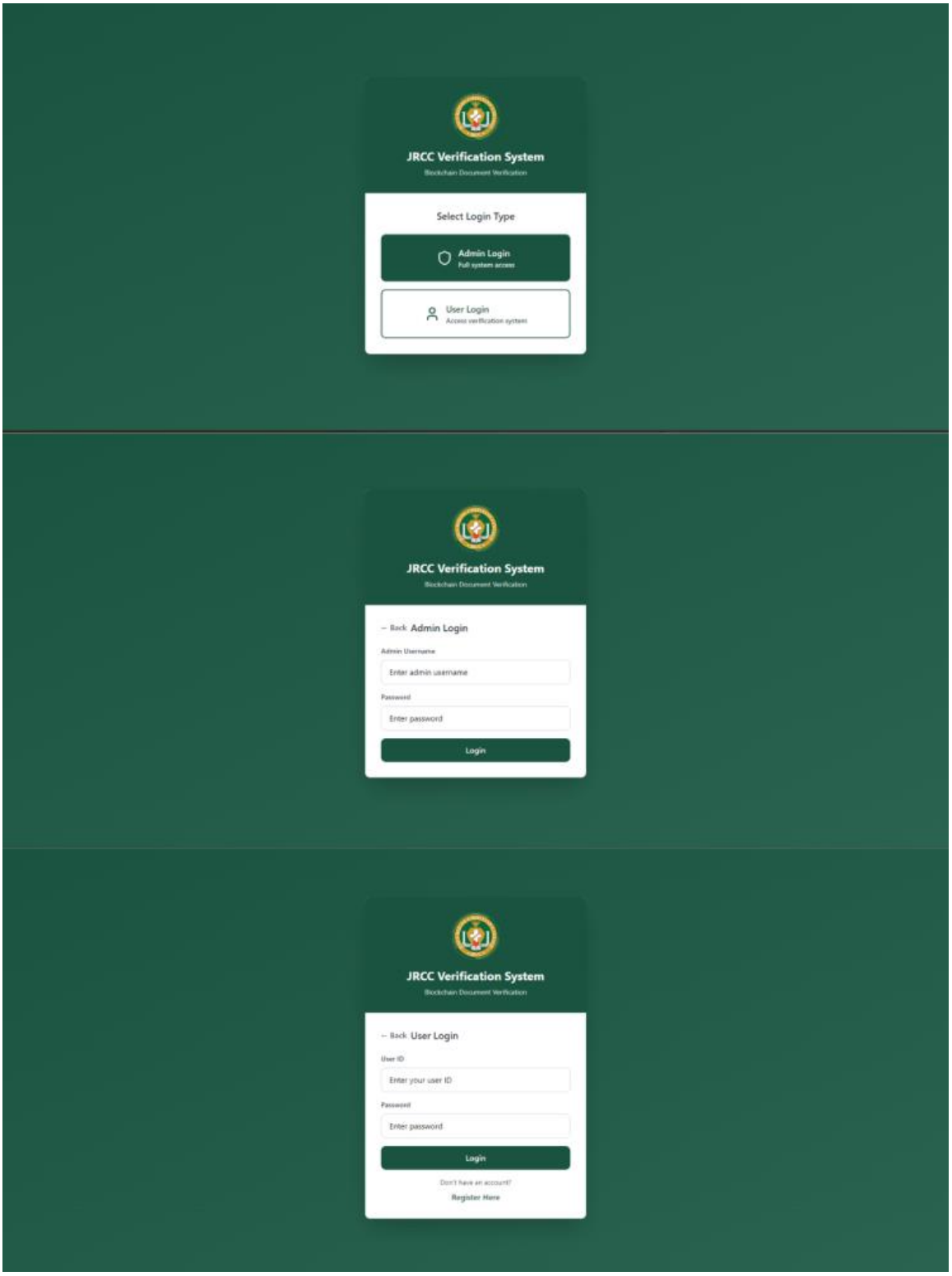

Figure 13. Login Page

Figure 13 presents the login interface of the JRCC Verification System. It serves as the entry point of the system and provides secure access for both administrators and users. The interface includes two login options: Admin Login and User Login. The Admin Login allows administrators to manage the system and monitor verification records, while the User Login enables users to access the document verification features. The login pages require authorized credentials such as username, user ID, and password to ensure data security and prevent unauthorized access. Overall, the interface was designed to be simple, organized, and user-friendly for efficient system navigation.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

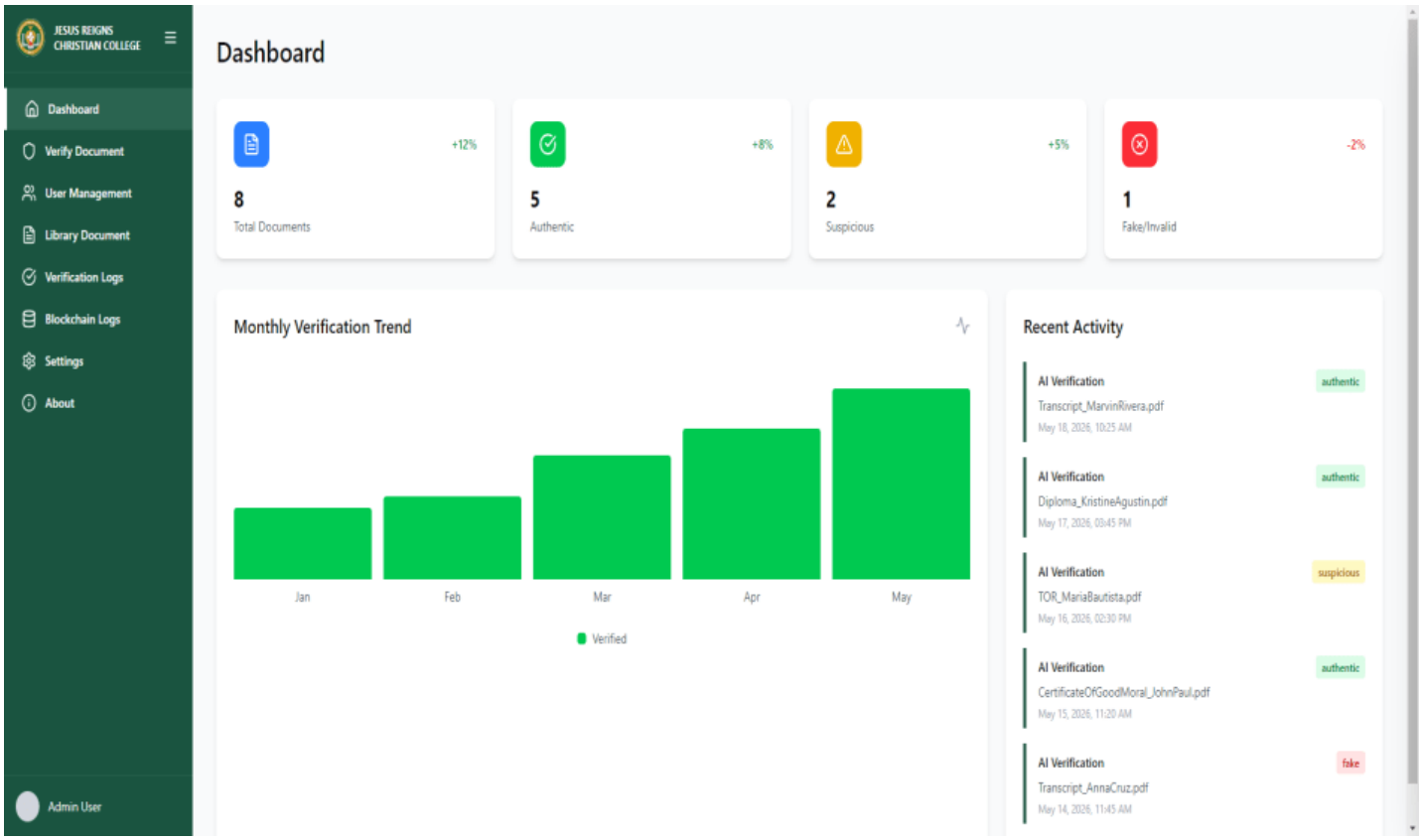

Figure 14. Dashboard Interface

Figure 14 presents the dashboard interface of the document verification system. The dashboard serves as the main monitoring panel where administrators can access and manage the overall verification activities of the system. It provides a summarized view of important information, including the total number of uploaded documents, authentic files, suspicious records, and fake or invalid documents processed by the system. These summary cards help administrators quickly evaluate the current status and performance of the document verification process.

The dashboard also includes a Monthly Verification Trend graph that visually represents the number of verified documents processed each month. This feature allows administrators to monitor system activity and analyze verification trends over a specific period of time. In addition, the Recent Activity section displays the latest document verification transactions, including document names, verification dates, and verification results. Through this feature, administrators can easily track recent system operations and identify documents that may require further checking or investigation.

Furthermore, the dashboard contains a navigation sidebar that provides easy access to other modules of the system, such as Verify Document, User Management, Library Documents, Verification Logs, Blockchain Logs, Settings, and About. Overall, the dashboard enhances the usability and efficiency of the system by presenting verification data in a clear, organized, and user-friendly interface.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

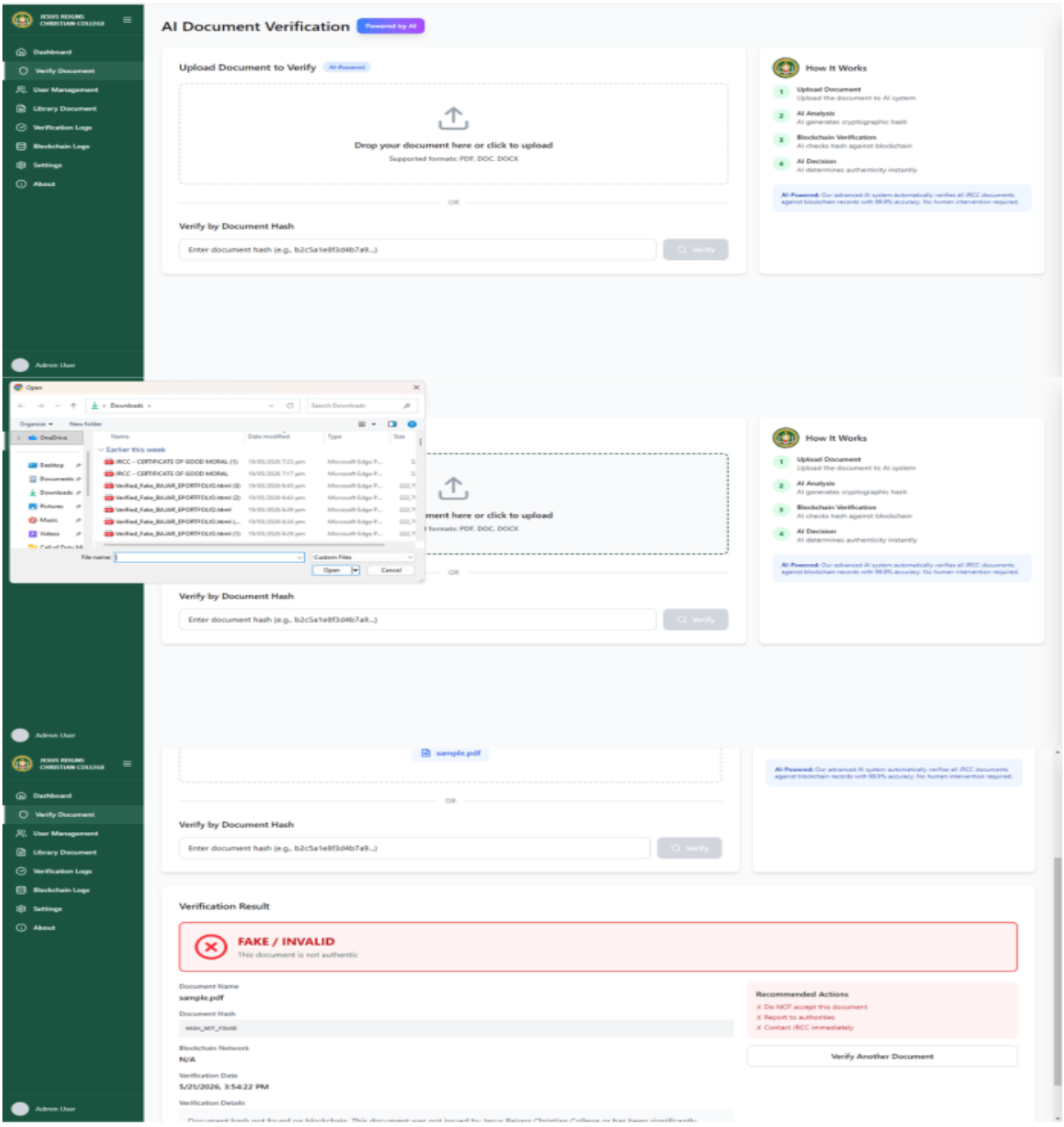

Figure 15. Verify Document Interface

Figure 15 presents the Verify Document interface of the document verification system. This module allows administrators or authorized users to upload documents for authenticity checking using the AI-powered verification process. Users can upload supported file formats such as PDF, DOC, and DOCX through the drag-and-drop upload section or by selecting files directly from their device. The interface also provides an alternative verification method through document hash input, where users can manually enter the document hash to verify its authenticity within the blockchain network.

The figure also shows the step-by-step verification process displayed in the “How It Works” panel, which includes document upload, AI analysis, blockchain verification, and AI decision-making. After the verification process is completed, the system generates a Verification Result section that displays the document status, such as authentic, suspicious, or fake/invalid. In the example shown, the uploaded document was identified as fake or invalid because the document hash was not found in the blockchain records. Additional details such as document name, verification date, blockchain network status, and recommended actions are also presented to guide administrators in handling suspicious or invalid documents properly.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

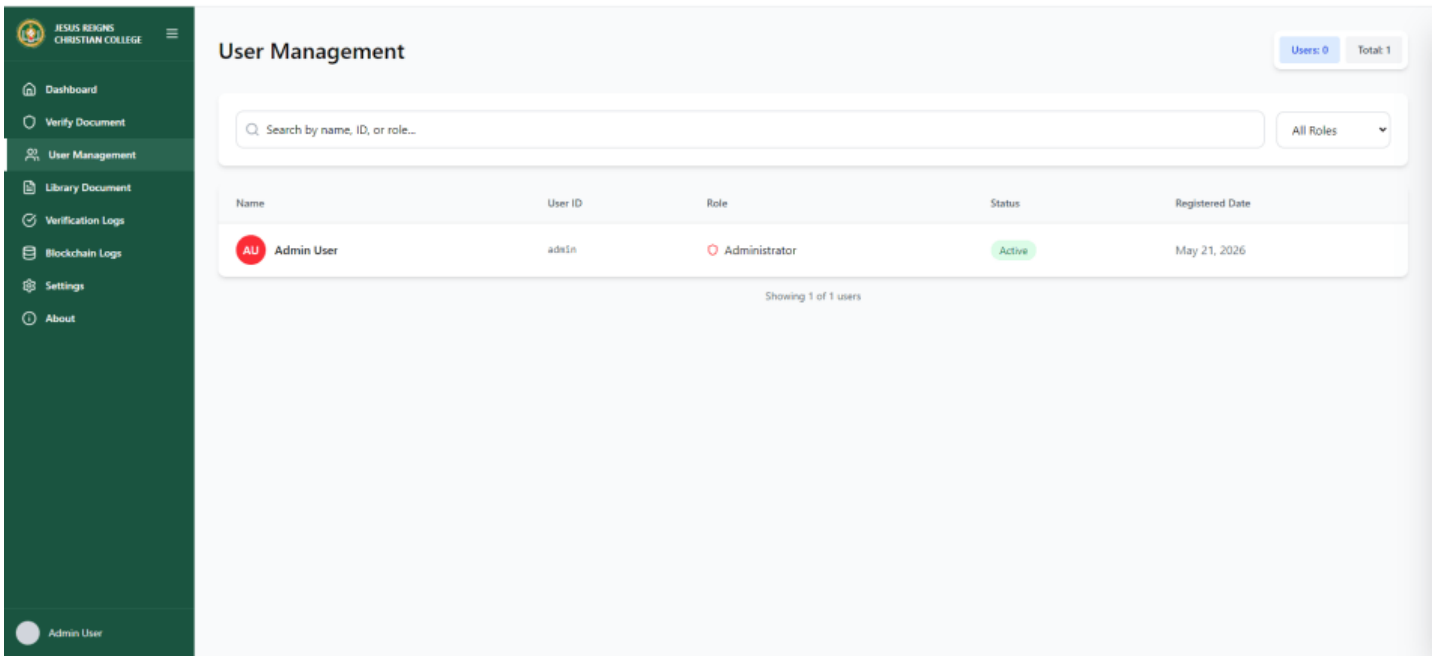

Figure 16. User Management Interface

Figure 16 shows the User Management Interface of the AI-Based Digital Document Authenticity Verifier. This module allows the administrator to manage and monitor registered users within the system. It displays user information such as name, user ID, role, account status, and registration date.

The interface also includes a search bar and role filter for easier user management and organization. This feature helps maintain secure system access and efficient administration of user accounts.

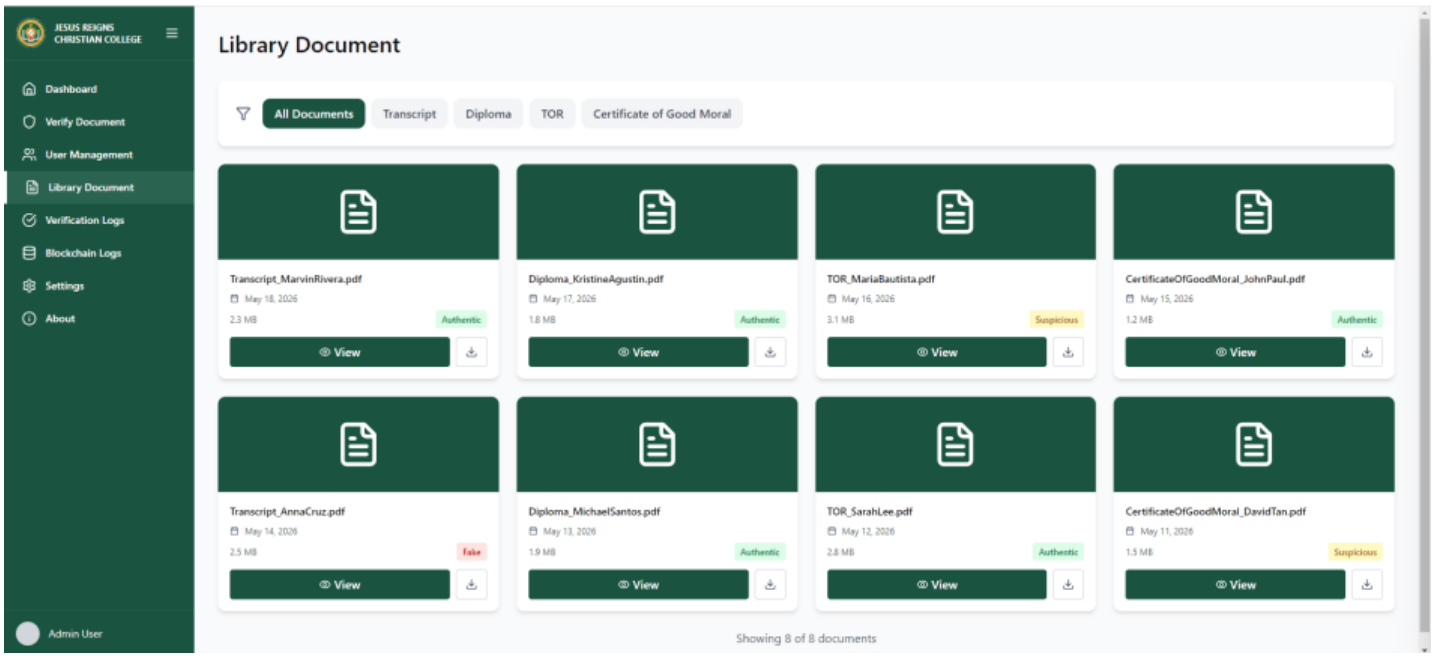

Figure 17. Library Document Interface

Figure 17 shows the Library Document Interface of the AI-Based Digital Document Authenticity Verifier. This module allows the administrator to view and manage stored academic documents within the system. The interface displays different document categories such as Transcript, Diploma, TOR, and Certificate of Good Moral. Each document record includes the file name, upload date, file size, and verification status such as Authentic, Suspicious, or Fake. The interface also provides options to view and download documents for easier document monitoring and management.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

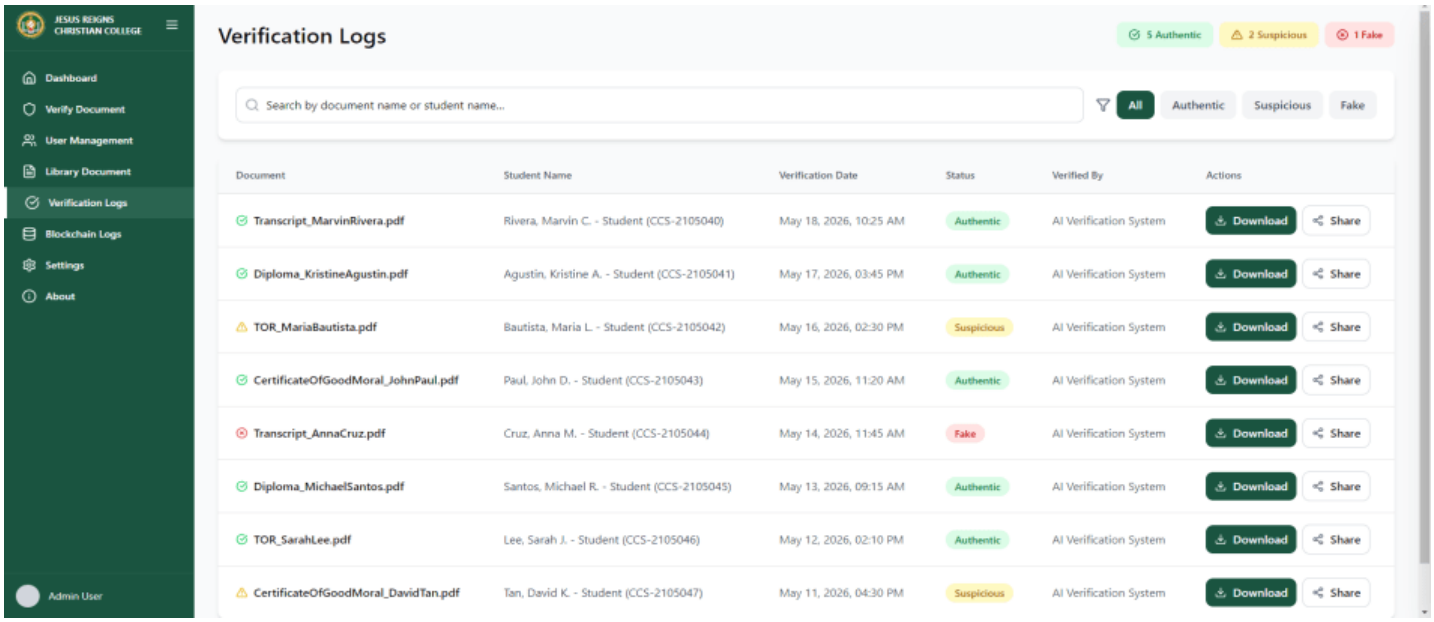

Figure 18. Verification Logs Interface

Figure 18 shows the Verification Logs Interface of the AI-Based Digital Document Authenticity Verifier. This module records and displays all verified documents processed by the system. The interface includes document name, student information, verification date, verification status, and verifier details. The system categorizes documents as Authentic, Suspicious, or Fake to help administrators easily monitor verification results. It also provides search, filtering, download, and sharing functions for efficient document tracking and management.

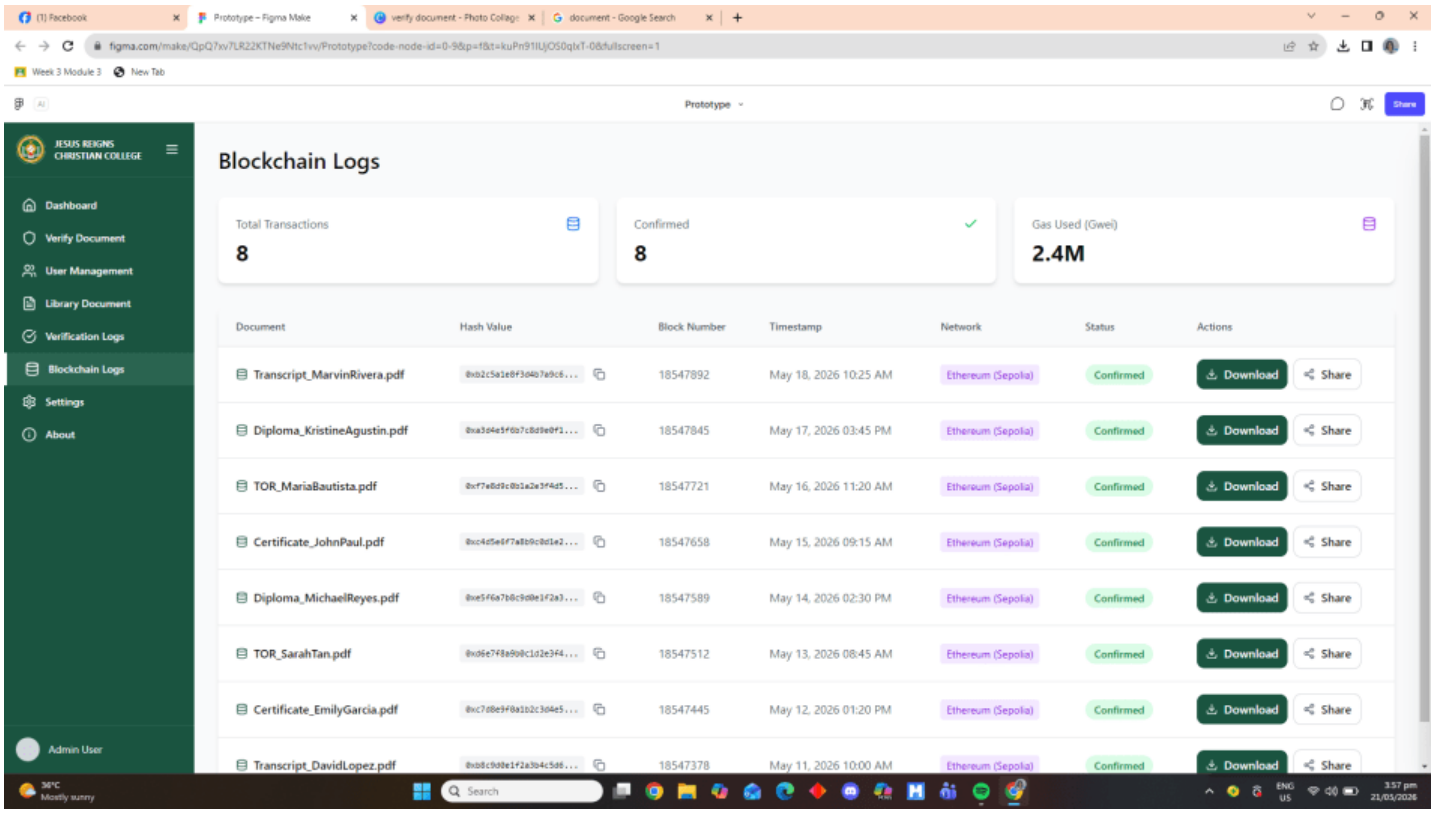

Figure 19. Blockchain Logs Interface

Figure 19 presents the Blockchain Logs interface, which serves as a centralized record-keeping module that logs all transactions and activities related to document processing within the system. This section displays essential summary data and detailed transaction entries, providing a clear and organized overview of every document registered and verified on the blockchain. It includes key information such as unique digital identifiers,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

timestamps, network details, and status updates, ensuring that all records are traceable, secure, and permanently stored. The interface also offers functional options for users to access or share documents, emphasizing transparency, accountability, and the integrity of stored academic records.

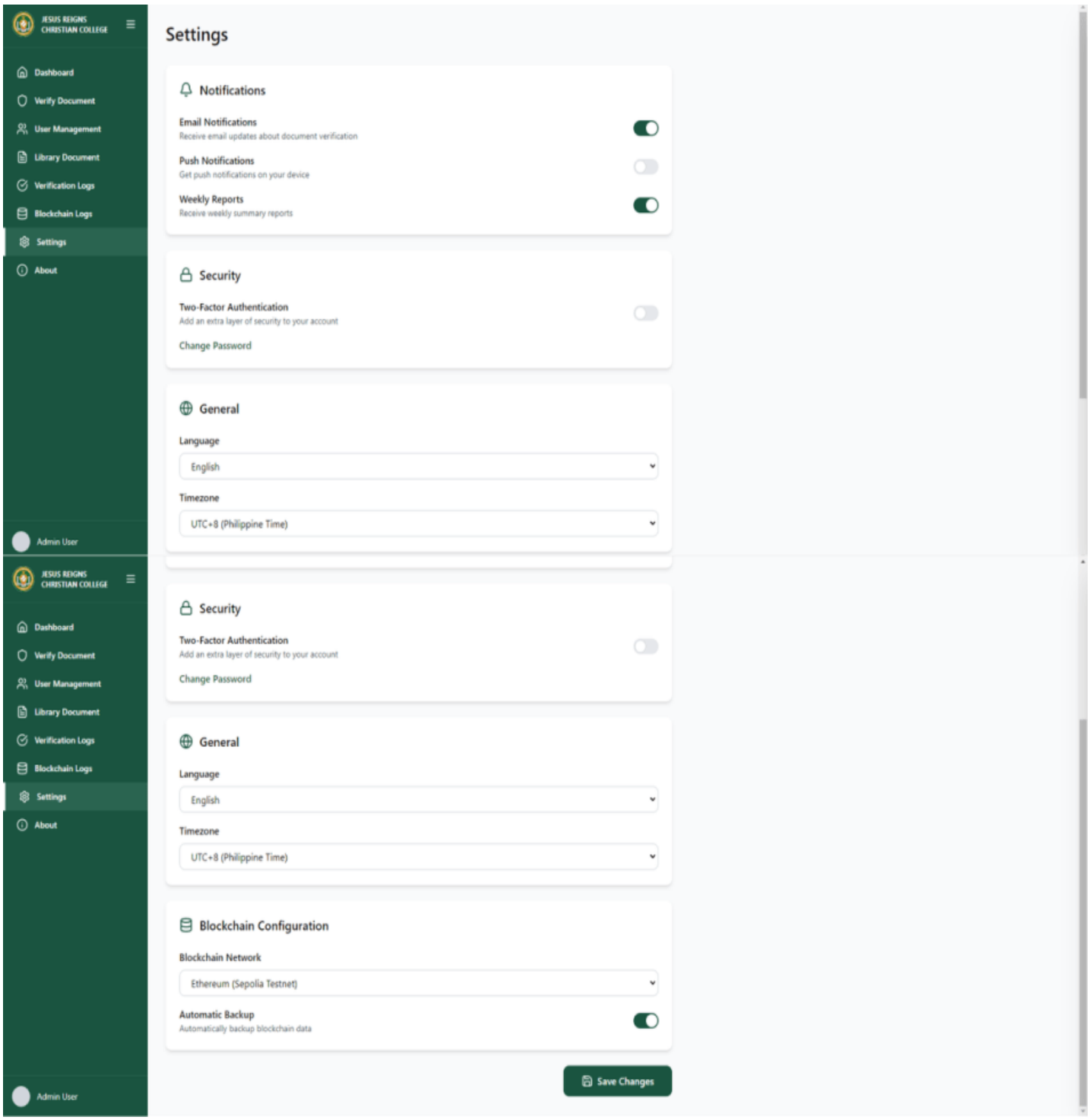

Figure 20. Settings Interface

Figure 20 displays the Settings module of the system, which serves as the central configuration panel allowing administrators to customize and manage system preferences according to operational requirements. This interface organizes options into distinct categories: Notifications for managing alerts and updates, Security for account protection measures, General for basic preferences such as language and time zone, and Blockchain Configuration for defining network parameters and data backup settings. It provides a structured and accessible way to adjust functionalities, ensuring the system operates in line with institutional standards, security protocols, and user requirements, while maintaining flexibility and control over core system behaviors.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

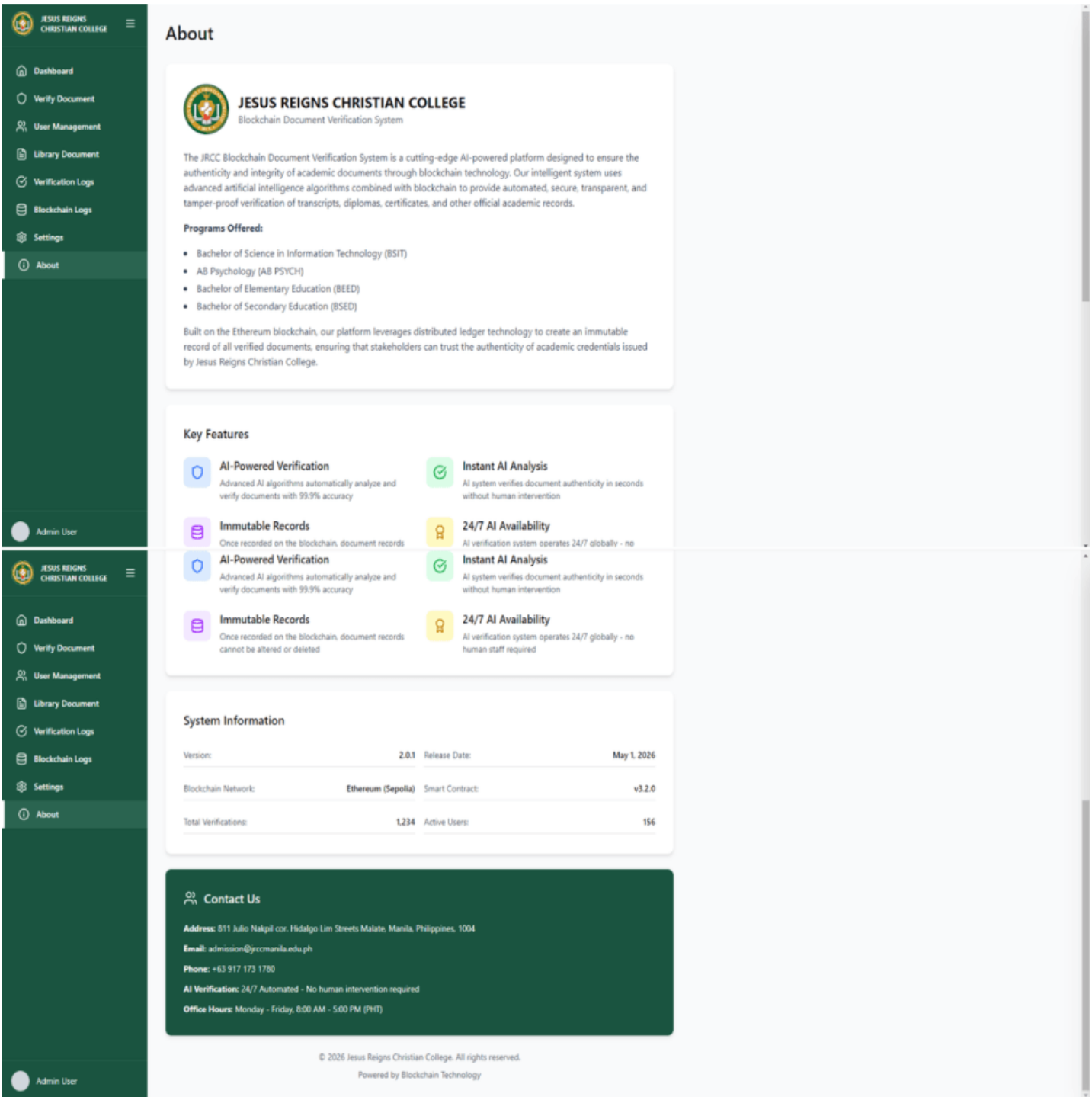

Figure 21. About Interface

Figure 21 displays the About interface, a dedicated informational section that provides a comprehensive overview of the platform, its purpose, and its underlying technology. It begins by introducing the institution and explaining the core objective of the system: to serve as a secure, advanced solution that leverages artificial intelligence and blockchain technology to guarantee the authenticity, integrity, and reliability of all academic documents and records. The section outlines the various academic programs offered by the college, emphasizing the scope of records managed by the platform. It further details the system's key features, such as automated verification processes, immutable record storage, real-time validation, and continuous accessibility, highlighting how these functionalities enhance efficiency, security, and trust in credential management. Additionally, this interface presents essential technical information including the system version, the specific blockchain network employed, and performance metrics, alongside complete institutional contact details and operational guidelines. Altogether, this page establishes transparency, reinforces the system's credibility, and clearly communicates its role in modernizing and securing the management of academic records within the institution.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

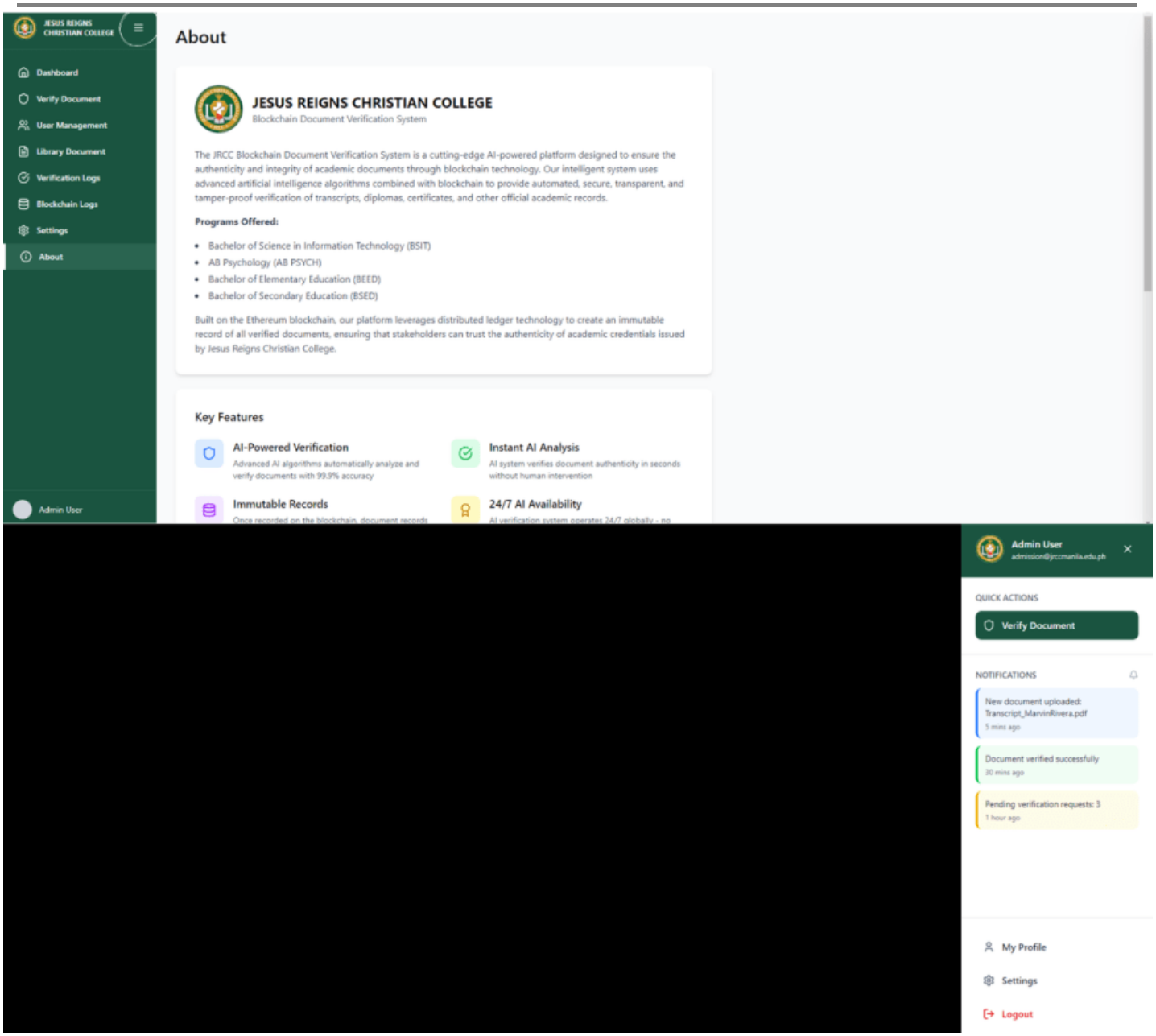

Figure 22. System Navigation

Figure 22 presents the standardized and consistent layout implemented throughout the entire administrator phase of the system, ensuring uniformity and ease of use across all functional modules and pages. Positioned prominently at the top left corner, directly adjacent to the official system logo, the hamburger menu remains constantly visible and accessible at all times; this essential navigation element serves as the primary control that allows authorized users to conveniently expand or collapse the main navigation sidebar, thereby providing instant and seamless access to various system features, management tools, and functional modules regardless of which page or screen is currently being viewed. On the opposite end of the header, located at the top right section of the interface, the user panel is clearly displayed, showing relevant account information, user credentials, and access details specific to the logged-in administrator. Integrated within this panel is the Logout function, distinctly marked with its recognizable icon for easy identification. Clicking this logo initiates a secure process that formally terminates and closes the current active session, ensuring that all access privileges are properly revoked, all ongoing operations are safely ended, and unauthorized access to sensitive data and system functions is effectively prevented. Upon successful execution of this action, the system automatically redirects the user and returns them directly to the main login interface, marking the completion of a secure session and requiring proper authentication once again to regain entry into the platform.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

System Users Phase

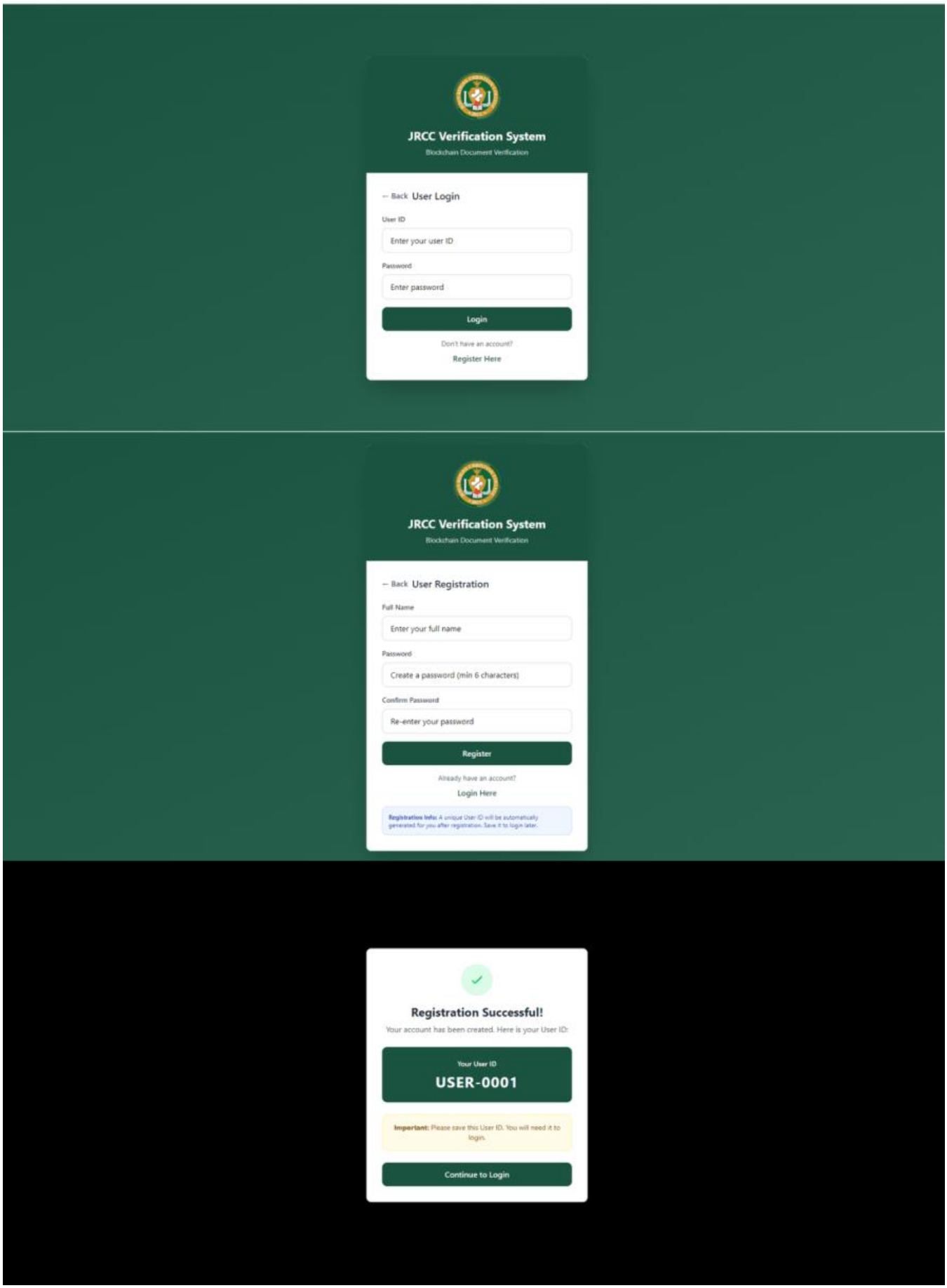

Figure 23. User Registration Interface

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Figure 23 illustrates the complete step-by-step user registration workflow designed to guide new users in creating a valid account within the JRCC Verification System. The first section displays the registration form, which serves as the initial step where users are required to provide essential information such as their full legal name and create a secure password that meets specified security standards, including a minimum character length. To prevent errors and ensure accuracy, the system includes a confirmation field where the password must be re-entered. Clear instructions are provided throughout the process, including a note informing users that a unique, system-generated User ID will be automatically assigned once registration is successfully completed. After submitting all required details and passing validation checks, the process moves to the confirmation stage, where a success message is displayed to verify that the account has been created and stored securely. This screen prominently presents the newly assigned unique User ID, serving as the official identifier for all future access, and includes an important reminder for the user to save this information for safekeeping. A dedicated button is also included to directly redirect the user to the login page, creating a seamless transition from account creation to system access. This structured workflow ensures that all new accounts are established with proper data validation, strong security measures, and a user-friendly experience, laying the foundation for secure and authorized usage of the platform.

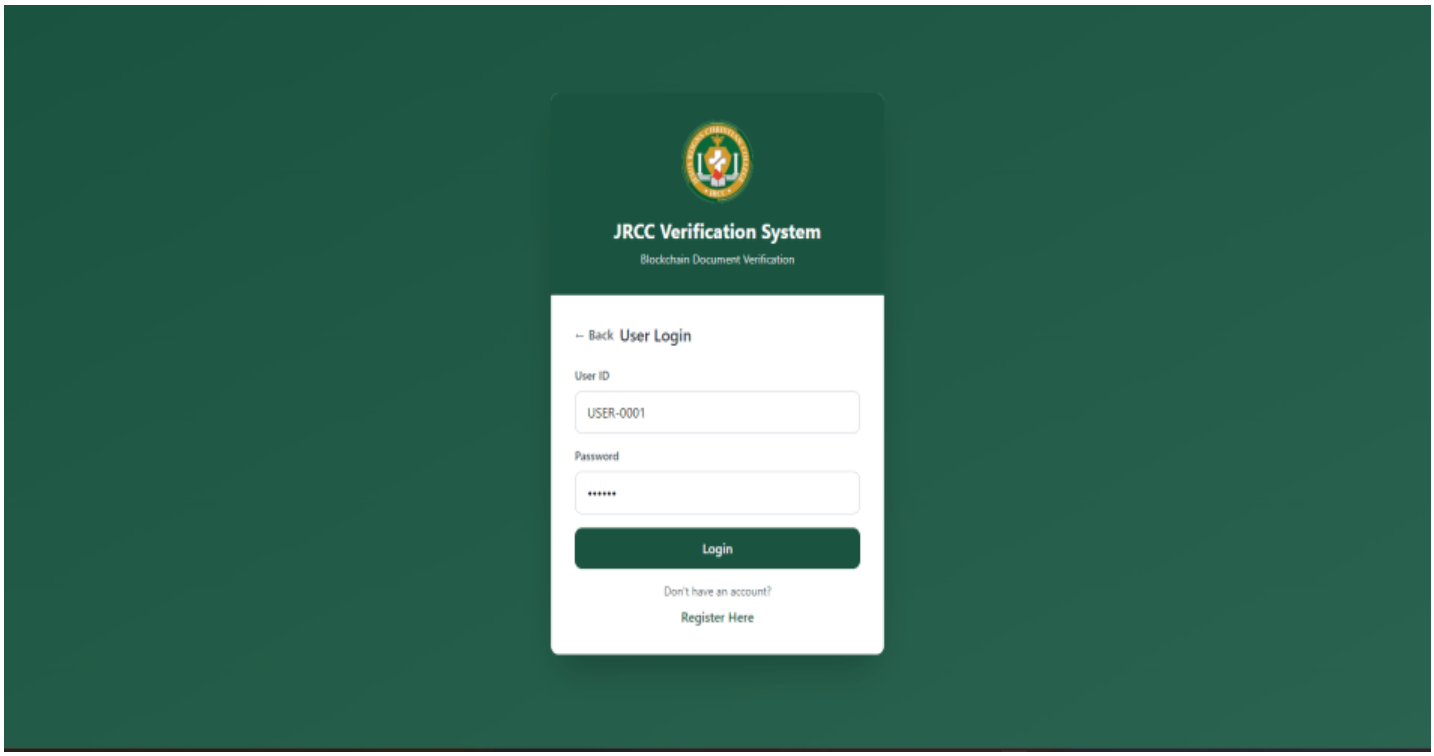

Figure 24. User Login Interface

Figure 24 presents the official login interface, which functions as the primary and secure entry point for all authorized users seeking to access the JRCC Verification System. The design is clean, professional, and clearly branded, prominently displaying the institution's official logo along with the full system name and its core function as a blockchain-powered document verification platform, reinforcing trust and institutional identity. At the center of the interface are two mandatory input fields: one for the unique User ID, which is assigned during registration, and another for the corresponding password. These two pieces of information serve as the fundamental authentication mechanism, ensuring that only individuals with valid and verified credentials are granted entry into the system. Once the correct details are entered and submitted, the system validates the information against stored records before allowing access to the dashboard and all administrative or verification features. Below the main login button, additional navigation options are provided for user convenience: a direct link labeled "Register Here" allows new users without an account to easily navigate to the registration page, while a "Back" option enables users to return to the previous screen if needed. This layout is designed to be intuitive and secure, establishing the first critical layer of access control, protecting sensitive data, and ensuring that every session begins with proper identity verification.

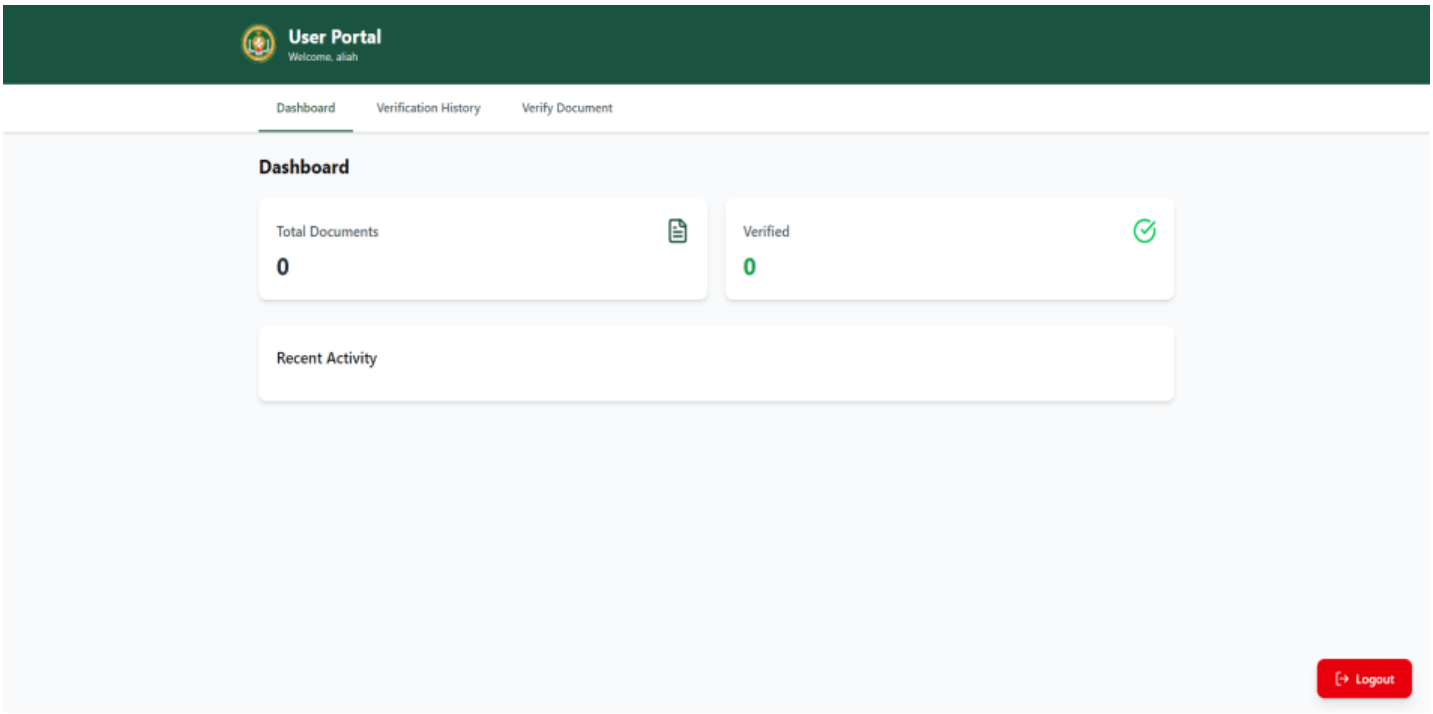

Figure 25. User Portal - Dashboard Interface

Figure 25 displays the main dashboard of the User Portal, serving as the central landing page and primary control center accessible immediately after a successful login. The interface features a clear and organized layout, starting with a header that identifies the section and greets the user, while a navigation menu provides direct access to key areas such as Dashboard, Verification History, and Verify Document. The main content presents essential information through summary cards showing the total number of documents and how many have been successfully verified, alongside a section dedicated to recent activity to keep users updated on the latest actions and transactions. A prominent logout button is positioned at the bottom right corner, allowing users to securely end their session and protect their account and data. This design offers a comprehensive yet simplified view of the user's status, combining important data, easy navigation, and security features to ensure efficient and secure management of documents and verification processes.

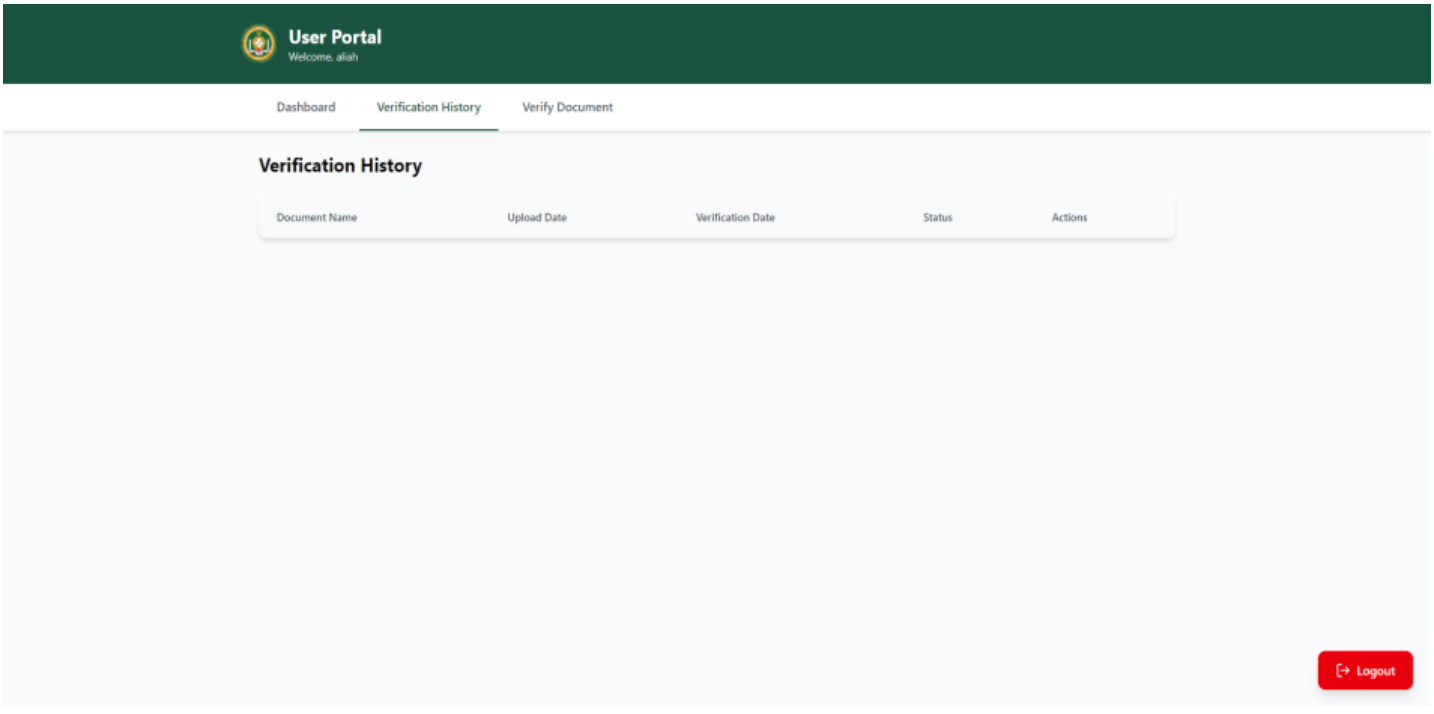

Figure 26. User Portal - Verification History

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Figure 26 shows the Verification History page within the User Portal, designed to provide users with a complete and organized record of all documents they have submitted for verification. The layout follows the same consistent structure, with a clear header and navigation bar to switch between Dashboard, Verification History, and Verify Document sections. The main feature of this page is a structured table with labeled columns: Document Name, Upload Date, Verification Date, Status, and Actions, intended to display detailed information about each submission, including when it was uploaded, when it was verified, its current status, and available options for further management. This section serves as a transparent log that allows users to easily track, review, and monitor the progress and outcome of every verification request they have made.

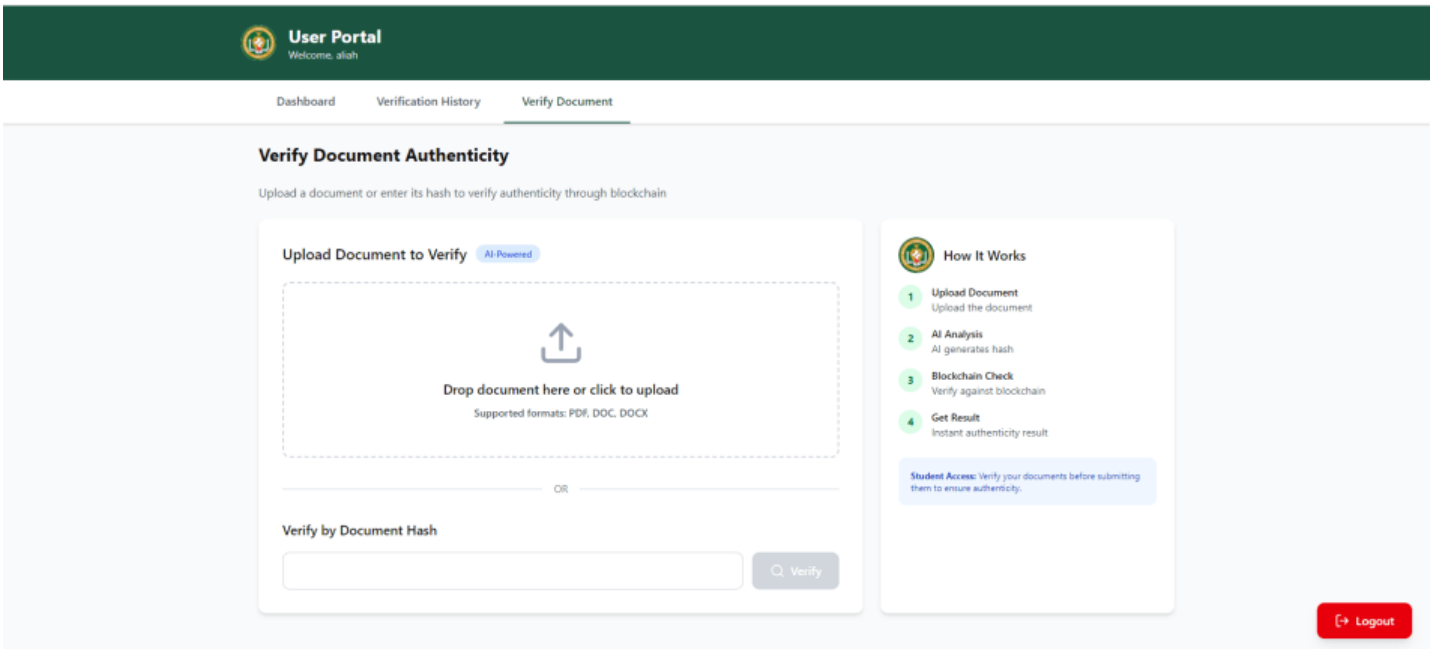

Figure 27. User Portal - Verify Document

Figure 27 shows the Verify Document section, the core feature of the portal used to check document authenticity. It offers two verification methods: uploading a file in supported formats or entering the document hash directly. A clear step-by-step guide on the right explains the process from upload to result. The navigation bar and logout button remain accessible, ensuring easy movement and secure session management.

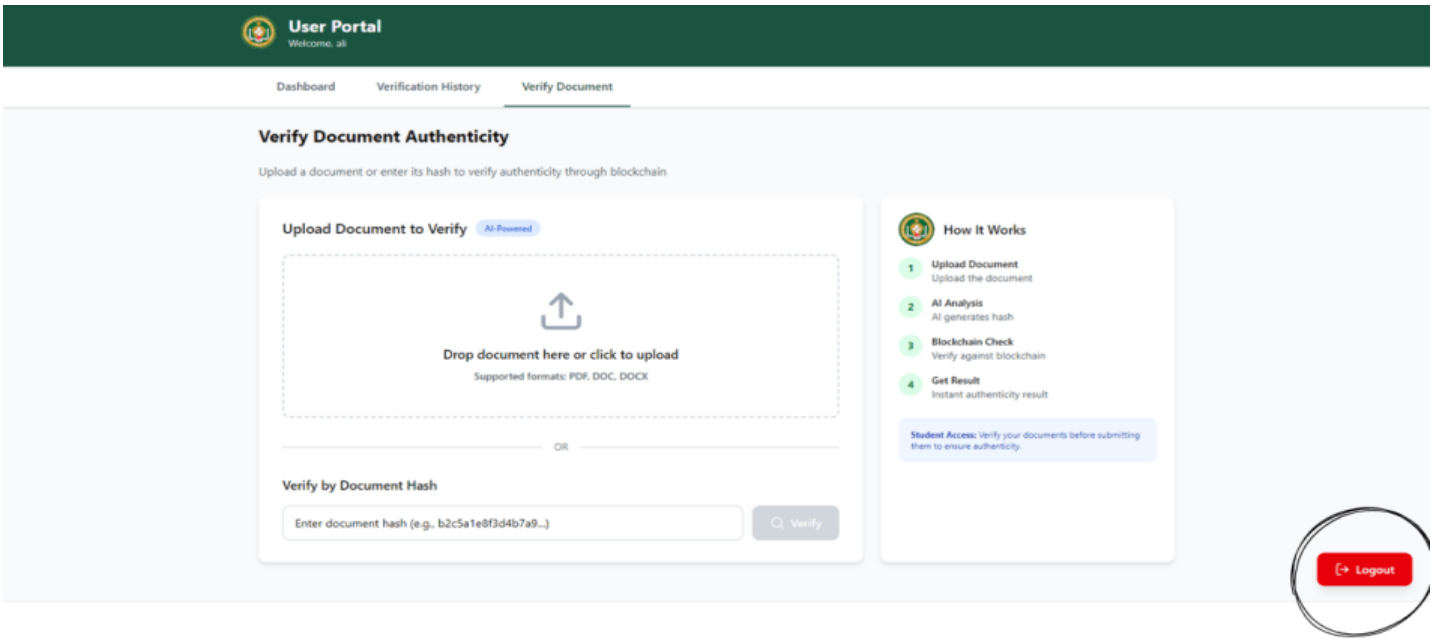

Figure 28. Logout Button

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Figure 28 shows a logout button positioned at the bottom right corner, this red button is visible on every interface throughout the system. Clicking it securely ends the active session and redirects the user back to the login page.

CONCLUSION

The study successfully developed an AI-Based Digital Document Authenticity Verifier designed to improve the verification of academic documents through artificial intelligence and cryptographic security methods. The system effectively detects document tampering by combining AI-based document analysis, SHA-256 hashing, and automated verification processes within a secure document management environment.

The results of the study showed that the system provides accurate, reliable, and efficient verification of digital documents. Through the integration of Gemini AI and SHA-256 hashing, the system was able to identify inconsistencies, detect unauthorized modifications, and maintain document integrity. The automated workflow also reduced manual verification efforts, minimized human error, and improved processing speed.

Furthermore, the implementation of features such as PDF report generation, blockchain logging, and secure document storage enhanced the overall reliability and credibility of the system. The study concludes that the developed system can serve as an effective solution for educational institutions in ensuring the authenticity and security of academic records and digital documents.

ACKNOWLEDGEMENT

The researchers would like to express their deepest gratitude and sincere appreciation to all individuals who contributed to the successful completion of this study entitled “AI-Based Digital Document Authenticity Verifier: Enhancing Document Security at Jesus Reigns Christian College.”

First and foremost, the researchers humbly thank Almighty God for His guidance, wisdom, strength, and countless blessings throughout the conduct of this study. His divine providence provided the researchers with perseverance and determination in overcoming the challenges encountered during the research process.

The researchers would also like to extend their heartfelt gratitude to the administrators, faculty members, and instructors of Jesus Reigns Christian College for their support, encouragement, and valuable insights that greatly contributed to the completion of this study. Special recognition is also given to the research adviser for the guidance, expertise, constructive suggestions, and continuous supervision provided throughout the development of the research.

Furthermore, the researchers express their sincere appreciation to their classmates, friends, and colleagues who provided encouragement, ideas, and motivation during the conduct of the study. Their support became an important part of the researchers’ academic journey.

The researchers are also deeply thankful to their families for their unwavering understanding, patience, moral support, and encouragement throughout the completion of this academic endeavor. Their inspiration motivated the researchers to persevere and successfully accomplish this study.

Lastly, the researchers extend their gratitude to everyone who directly or indirectly contributed to the realization and completion of this research study.

REFERENCES

1. Boonkrong, S. (2025). Design of an academic document forgery detection system. International Journal of Information Technology, 17, 5175–5187. https://doi.org/10.1007/s41870-024-02006-6
2. Darem, A., Al-Hashmi, A., Javed, M., & AbuBaker, B. A. (2020). Digital forgery detection of official document images in compressed domain. International Journal of Computer Science and Network Security, 20(12), 115–123. https://doi.org/10.22937/IJCSNS.2020.20.12.12

3. Jagtap, A., Sawat, D. D., & Hegadi, R. S. (2020). Verification of genuine and forged offline signatures using Siamese Neural Network (SNN). Multimedia Tools and Applications, 79(1). https://doi.org/10.1007/s11042-020-08857-y
4. Rane, M., Singh, S., Singh, R., & Amarsinh, V. (2020). Integrity and authenticity of academic documents using blockchain approach. ITM Web of Conferences, 32, 03038. https://doi.org/10.1051/itmconf/20203203038
5. Sirajudeen, M., Anitha, R., Varadarajan, V., Kommers, P., Piuri, V., & Subramaniyaswamy, V. (2020). Forgery document detection in information management system using cognitive techniques. Journal of Intelligent & Fuzzy Systems, 39(6), 8057–8068. https://doi.org/10.3233/JIFS-189128
6. Wang, X., Pang, S., Qiao, S., & Lv, Z. (2023). TVS: A trusted verification scheme for office documents based on blockchain. Complex & Intelligent Systems, 9, 2865–2877. https://doi.org/10.1007/s40747-021-00617-1
7. Wei, J., Chen, H., & Zhang, Y. (2021). Authenticity verification on social data outsourcing. Computers & Security, 100, 102077. https://doi.org/10.1016/j.cose.2020.102077
8. Aldwairi, M., Badra, M., & Borghol, R. (2023). DocCert: Nostrification, document verification and authenticity blockchain solution. arXiv. https://arxiv.org/abs/2310.09136
9. Vinogradov, A. (2026). Can generative models actually forge realistic identity documents? arXiv. https://arxiv.org/abs/2601.00829
10. Mohit, A., Aggarwal, B., & Gondhalekar, C. (2026). Provenance verification of AI-generated images via a perceptual hash registry anchored on blockchain. arXiv. https://arxiv.org/abs/2602.02412