Blockchain-Enabled Smart Library Management with RFID and Biometric Access Control

Mr.N. Ramakumar, B.Vijay Kumar Reddy, M. Venkata Sathish, G.Y. Veera Reddy, T.Vivek

Aditya College of Engineering, Madanapalle.

Abstract: This paper presents the design and development of an advanced Smart Library Management System aimed at enhancing the automation, security, and transparency of library operations. Traditional library systems largely depend on manual record-keeping and physical identification cards, which are susceptible to human error, loss, and unauthorized usage. Moreover, the design of distributed databases is likely to result in opacity of operations and the potential for data forgery. The current system utilizes RFID, biometrics, and Blockchain to improve the security of data entry and access. As an entry-authentication reader, the MFRC522 collects and registers each entry of a book tagged with a passive RFID, streamlining the entry and exit of books in the system. The biometric sensor is a fingerprint scanner, and this biometric security technology ensures that people unauthorized to use the library and books cannot access the library and books, except for the use of a library operator ID card. The edge computing actuator is a Raspberry Pi 4, and it collects and sends data to the cloud server for the system to provide library services via SMS in response to the control system's relay switch. The server, as the software component, is a web application designed with the Flask framework, and it provides end-to-end services for the library management system, and it contains modules for the management of users, books, and transactions. Additionally, cloud computing is employed to ensure the database is optimized for storage and retrieval operations. Each activity that is performed in the system is recorded to ensure data integrity and provide a reliable network of trust for the library management system. The effectiveness and efficiency of the proposed system is established via its experimental outcomes.

Index Terms: Blockchain technology, Hyperledger Fabric, Smart library, Fingerprint sensor, RFID, Supabase database.

I. INTRODUCTION

Libraries play a vital role in supporting academic, research, and knowledge-sharing activities. However, many conventional library management systems continue to rely on manual processes and centralized digital solutions that are often inefficient, time-consuming, and vulnerable to security risks. Tasks such as book issuance, return tracking, and user authentication typically depend on physical identification cards and manual record-keeping, which can lead to errors, delays, and unauthorized access. Moreover, centralized databases, while widely adopted, lack transparency and are susceptible to data manipulation, raising concerns about the integrity and reliability of library records.

Technological developments aimed at the Internet of Things (IoT), biometric authentication, and blockchain in recent years have proven useful in system modernization and security. Radio Frequency Identification (RFID) technology., in particular, has gained significant attention in library automation due to its ability to enable fast, contactless identification of books and resources. Similarly, biometric authentication methods, such as fingerprint recognition, offer a robust mechanism for verifying user identity, eliminating the limitations associated with physical ID cards. While these technologies improve efficiency and access control, they do not inherently address the issue of data immutability and trust in centralized systems.

Blockchain technology, especially permissioned frameworks, provides a promising solution to these challenges by enabling decentralized, transparent, and tamper-resistant record management. By recording transactions in an immutable distributed ledger, blockchain ensures that once data is validated and stored, it cannot be altered or deleted, thereby enhancing accountability and trust. Integrating blockchain with RFID and biometric systems can significantly strengthen the overall security and reliability of library operations.

Motivated by these advancements, this paper proposes a Blockchain-Enabled Smart Library Management System that combines RFID-based book identification, biometric user authentication, and a permissioned blockchain network to create a secure and automated library ecosystem. The system leverages an edge computing platform to coordinate hardware components and integrates a web-based interface for efficient management of library resources and user activities. By recording all transactions on a blockchain ledger, the proposed approach ensures data integrity, transparency, and auditability. The remainder of this paper presents the system design, implementation, and evaluation of the proposed solution, demonstrating its effectiveness in improving operational efficiency, enhancing security, and providing a reliable and user-friendly library management experience.

II. LITERATURE SURVEY

The evolution of library management systems has been significantly influenced by advancements in automation, identification technologies, and secure data management frameworks. Early research primarily focused on improving operational efficiency through the adoption of Radio Frequency Identification (RFID) technology. For instance, Polycarpou et al. [1] demonstrated the feasibility of RFID-enabled smart cabinets for automated book

handling, highlighting improvements in tracking accuracy and inventory management. Similarly, Nawi et al. [2] and Singh and Sharma [3] developed intelligent RFID-based systems that streamlined book issuance and return processes, reducing manual intervention and enhancing overall efficiency. Additional studies [9], [11], and further reinforced the effectiveness of RFID in minimizing human error and enabling contactless identification within library environments.

While RFID significantly improved automation, researchers identified limitations related to user authentication and system security. To address these concerns, biometric technologies were introduced as a reliable method for identity verification. Afolabi and Aruna [4] proposed a bimodal biometric approach to secure e-library systems, demonstrating improved resistance to unauthorized access. Likewise, Kumar and Rani [10] emphasized the role of biometric authentication in strengthening access control mechanisms. Foundational work by Jain et al. established the robustness of biometric recognition systems, particularly fingerprint-based methods, in providing accurate and secure user identification. Furthermore integrated biometric authentication with IoT-based smart library systems, illustrating enhanced security and user accountability.

The integration of Internet of Things (IoT) technologies has also played a crucial role in modernizing library systems. Desai et al. [5] proposed an IoT-based smart library framework that enabled real-time monitoring and management of library resources. Such systems leverage interconnected devices to facilitate seamless communication between hardware components and software platforms, improving responsiveness and operational efficiency. However, despite these advancements, most IoT-based and RFID-enabled systems continue to rely on centralized databases, which remain vulnerable to data tampering and lack transparency.

To overcome these limitations, recent research has explored the application of blockchain technology in library and educational systems provided a comprehensive overview of blockchain architecture and its potential for ensuring data integrity through decentralized consensus mechanisms. Androulaki et al. [7] introduced Hyperledger Fabric as a permissioned blockchain framework capable of supporting secure and scalable enterprise applications. Complementing this, Barger et al. [6] proposed a Byzantine fault-tolerant consensus mechanism to enhance the reliability of blockchain networks. More recent studies [8] have investigated blockchain applications in education and library systems, emphasizing its ability to provide immutable record-keeping, transparency, and trust.

Despite the significant progress achieved in RFID, biometric, IoT, and blockchain technologies individually, there remains a gap in fully integrated systems that combine all these components into a unified framework. Most existing solutions address either automation, authentication, or data security in isolation, without providing a comprehensive approach to all three aspects simultaneously.

Motivated by these observations, the present work aims to bridge this gap by proposing a Blockchain-Enabled Smart Library Management System that integrates RFID-based book identification, biometric user authentication, and a permissioned blockchain network. This integrated approach ensures not only efficient automation and secure access control but also guarantees data immutability, transparency, and auditability, thereby addressing the limitations of existing systems.

III. PROPOSED METHOD

This work proposes a Blockchain-Enabled Smart Library Management System that unifies RFID-based book identification, biometric user authentication, and a permissioned blockchain network to deliver a secure, transparent, and fully automated library environment. The system is designed to eliminate manual intervention, prevent unauthorized access, and ensure the integrity of all transactions through an immutable audit trail.A three layer distributed architecture has been proposed for SDN. The three layers are categorized as Core Layer, Distribution Layer and Access Layer. The Core layer having two Core Switches is configured as the nucleus of the network and is intended to provide means for information exchange between various systems like ACCS and CMS. The Access layer having a myriad of Ethernet Edge Switches is the outermost layer and is intended to provide connectivity to the end equipment of all systems like ACCS and CMS. The Distribution layer having two dedicated distribution switches for each system (ACCS and CMS) is positioned between the Core layer and the Access Layer providing connectivity Between two layers.

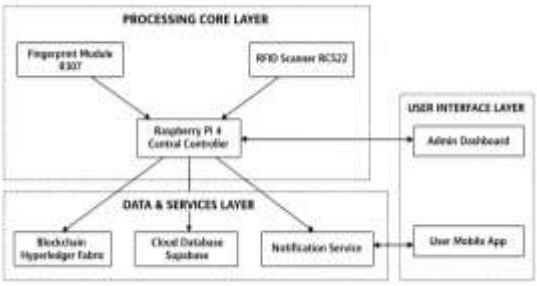

Figure 1: Proposed System Block Diagram

System Overview:

The architecture follows a layered approach comprising (i) a hardware layer for sensing and identification, (ii) an edge computing layer for coordination and control, (iii) an application layer for user interaction and administration, and (iv) a blockchain layer for secure and tamper-resistant record management. These layers are tightly integrated to enable real-time operation, reliable data exchange, and end-to-end security.

Hardware and Edge Layer:

At the hardware level, each book is equipped with a passive RFID tag, which stores a unique identifier. An MFRC522 RFID reader is deployed at the circulation desk

to enable rapid, contactless scanning of books during issuance and return. For user authentication, a fingerprint-based biometric sensor is integrated into the system, ensuring that only registered users can access services. This approach removes dependence on physical library cards and significantly reduces the risk of identity misuse.

A Raspberry Pi 4 functions as the edge computing unit, interfacing with the RFID reader and biometric sensor. It manages device-level operations, performs initial data validation, and orchestrates communication with the backend services. By processing requests at the edge, the system reduces latency and maintains reliable operation even under intermittent network conditions.

Application and Data Management Layer:

The software component is implemented as a web-based application using the Flask framework, providing a clean and intuitive interface for librarians and administrators. The application supports core functionalities such as user registration, biometric enrollment, book catalog management, and transaction monitoring. It also enables real-time status updates for issued and returned books.

A cloud-hosted database is employed to store operational data, including user profiles, book metadata, and system logs. This ensures fast data retrieval and scalability while supporting concurrent access. The application layer interacts seamlessly with both the edge device and the blockchain network through secure APIs, maintaining consistency across the system.

Blockchain Integration Layer:

To address concerns related to data integrity and trust, the system incorporates a permissioned blockchain network based on Hyperledger Fabric. Every valid transaction, including book issuance and return events, is submitted to the blockchain through a custom smart contract (chaincode). Transactions are verified by designated endorsing peers before being committed to the distributed ledger.

Once recorded, each transaction becomes immutable and cannot be altered or deleted, thereby establishing a tamper-proof audit trail. Only the transaction hash and essential metadata are stored on-chain, while detailed records remain in the off-chain database, ensuring efficient storage utilization. This hybrid approach balances performance with security, providing both transparency and scalability.

Notification and User Interaction:

To enhance user experience, the system incorporates a real-time notification mechanism that alerts users about successful transactions, due dates, and system updates. Notifications are delivered instantly, ensuring that users remain informed about their library activities and reducing the likelihood of overdue returns.

Operational Workflow:

The system operates through a streamlined workflow. A user first undergoes biometric authentication to gain access. Upon successful verification, books are scanned using the RFID reader. The system validates the transaction, updates the database, and simultaneously records the event on the blockchain network. Once confirmed, the transaction is finalized, and a notification is sent to the user. The same process applies to book returns, ensuring consistency and traceability across all operations.

Key Features and Advantages:

The proposed system offers several advantages over conventional library management solutions. It ensures secure access through biometric authentication, enables fast and accurate book handling using RFID, and guarantees data integrity through blockchain technology. The integration of edge computing enhances responsiveness, while the web-based interface simplifies system management. Overall, the solution provides a reliable, scalable, and future-ready platform for modern library environments.

IV. PROPOSED FLOW CHART

The flowchart illustrates the operational workflow of the Blockchain-Enabled Smart Library Management System with RFID and Biometric Access Control, highlighting the sequence of processes from user entry to transaction completion and notification. The system is designed to ensure secure access, efficient book handling, and reliable transaction recording through an integrated architecture.

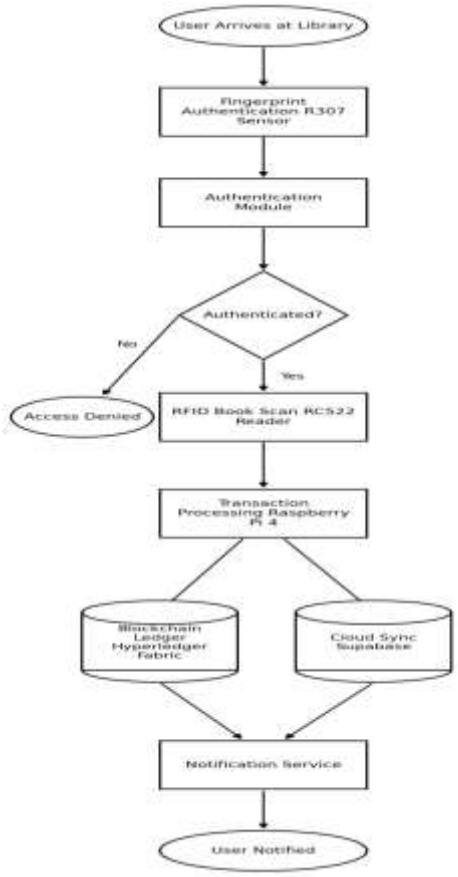

Figure 2: Proposed System Flowchart

The process begins when a user arrives at the library. To initiate access, the user is required to undergo biometric verification using a fingerprint sensor (R307). This step serves as the primary authentication mechanism, replacing traditional identification methods such as library cards. The captured fingerprint data is processed by the authentication module, which verifies the user's identity against pre-registered records.A decision point follows this stage, determining whether the authentication is successful. If the authentication fails, access is immediately denied, thereby preventing unauthorized usage of library resources. This ensures a high level of security and eliminates the risk of identity misuse. Conversely, if the authentication is successful, the system proceeds to the next stage of operation.

Upon successful verification, the user is allowed to scan books using the RC522 RFID reader. Each book is equipped with a passive RFID tag containing a unique identifier, enabling quick and contactless scanning. This significantly reduces the time required for issuing or returning books and minimizes human intervention.The scanned data is then transmitted to the Raspberry Pi 4, which functions as the central processing unit of the system. At this stage, transaction processing takes place, where the system determines whether the operation corresponds to a book issue or return. The Raspberry Pi coordinates communication between the hardware components and backend services, ensuring seamless data flow.

Following transaction processing, the system simultaneously updates two key components: the blockchain ledger and the cloud database. The transaction details are securely recorded on a blockchain network, ensuring immutability and transparency. This creates a tamper-proof audit trail of all library activities. In parallel, the data is synchronized with a cloud-based database, enabling efficient storage, retrieval, and management of records.Once the transaction is successfully recorded and synchronized, the system triggers a notification service. This module sends real-time alerts to the user, informing them of successful book issuance or return, along with any relevant details. The process concludes with the user receiving confirmation, thereby completing the transaction cycle.

Overall, the flowchart demonstrates a well-structured and secure workflow that integrates biometric authentication, RFID-based automation, edge computing, blockchain technology, and cloud services. This cohesive approach enhances operational efficiency, strengthens security, and ensures transparency in library management processes.

Web Dashboard and User Interface:

The web dashboard functions as the primary interface for both end users and administrators, providing a unified platform for interacting with the smart library system. It is designed to integrate seamlessly with the backend services, enabling efficient management and real-time monitoring of library operations. The frontend is developed using standard web technologies, including HTML, CSS, and JavaScript, resulting in a lightweight, responsive, and device-independent interface. The application is served through a Flask-based backend, which also exposes a set of APIs to handle data exchange and system operations.

To enhance user experience and ensure smooth interaction, the dashboard employs asynchronous JavaScript techniques (AJAX). This allows dynamic data retrieval and updates without requiring full page reloads, thereby enabling real-time responsiveness and improving overall usability. The interface is structured into multiple functional modules, each addressing a specific aspect of the library system.

The Real-time Statistics module provides live insights into system performance, including book circulation patterns,user activity, and operational status. This feature enables administrators to monitor library usage and make informed decisions based on up-to-date information.

The User Registry Management module allows administrators to efficiently manage user records. It supports the addition, modification, and removal of users, while securely linking biometric data to individual profiles for accurate identification and access control.

The Book Inventory Management module offers comprehensive tools for maintaining the library's catalog. It facilitates the tracking, updating, and synchronization of book records, ensuring that all RFID-tagged items are accurately reflected in the system database.

The Transaction History module maintains a detailed and immutable record of all book issuance and return activities. These records are synchronized with the blockchain ledger, ensuring transparency, traceability, and protection against data tampering.

Finally, the System Audits module enables administrators to review blockchain-based logs and verify the integrity of recorded transactions. This feature supports accountability by allowing the detection of anomalies and ensuring that all operations comply with system protocols.

Overall, the web dashboard provides a cohesive and intuitive interface that enhances system usability while supporting secure, transparent, and efficient library management.

V.SIMULATION RESULTS

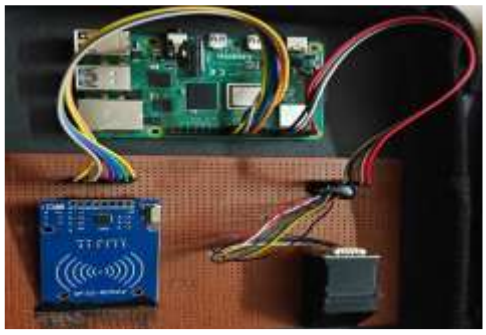

Figure 3: Experimental Setup

Figure 4: Entry Authentication Success Screenshot

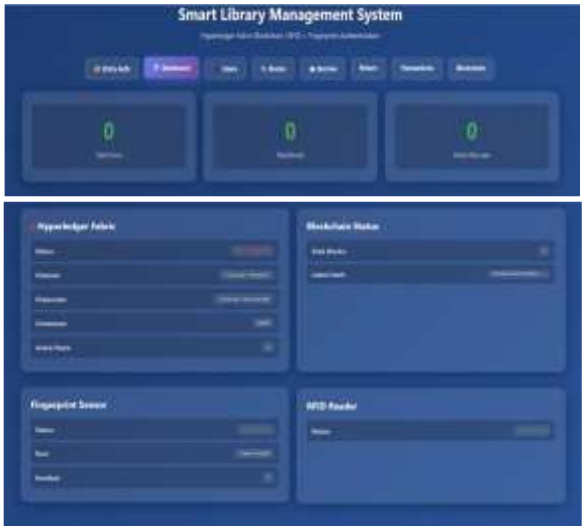

Figure 5: Web Dashboard Overview Screenshot

Figure 6: Book Borrow Transaction

Figure 7: Book Return Transaction

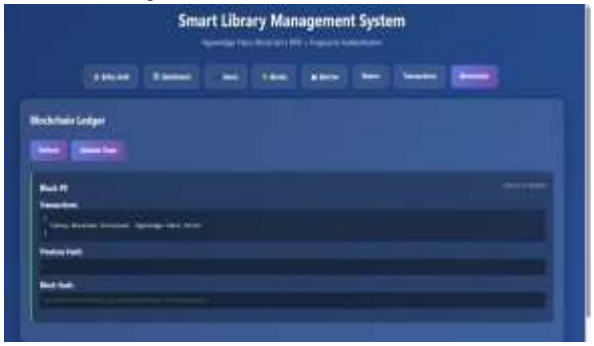

Figure 8: Blockchain Verification Status

Figure 10: Ntfy Push Notification Delivery on Mobile Device

VI CONCLUSION

This study successfully presents the design and implementation of a Smart Library Management System that effectively overcomes the limitations associated with traditional library operations. By integrating MFRC522 RFID technology, the system enables fully automated identification and tracking of books, thereby eliminating the need for manual barcode-based processes and significantly improving operational efficiency.The incorporation of optical fingerprint-based biometric authentication replaces conventional physical identification cards, which are often prone to loss or misuse. This enhancement ensures that only authorized users can access library services and perform transactions, thereby strengthening access control and overall system security.

In addition, the integration of a Hyperledger Fabric-based blockchain network elevates the system's reliability and trustworthiness. By recording each borrowing and return transaction on a distributed ledger, the system guarantees data immutability and prevents unauthorized modifications. This blockchain-backed approach establishes a transparent and tamper-resistant audit trail, enhancing accountability in library operations.

REFERENCES

1. C. Polycarpou, T. Samaras, and J. N. Sahalos. (2014, April). An RFID-based library management system using smart cabinets: A pilot project. 8th European Conference on Antennas and Propagation (EuCAP 2014), The Hague,

Netherlands, pp. 106- 108. https://doi.org/10.1109/EuCAP.2014.6902447

2. M. R. M. Nawi, M. F. A. Rahman, and M. I. M. Rawi. (2021, August). Intelli gent RFID Based Library Management System. 2021 IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 1- 5. https://doi.org/10.1109/ICCCA52192.2021.9622566
3. S. K. Singh and A. K. Sharma. (2024, February). Library Management System using RFID. International Journal of Computer Applications (IJCA), vol. 175, no. 10, pp. 12- 16.
4. O. Afolabi and M. A. Aruna. (2020). Securing E-Library System with Bimodal Biometric Technique. Archives of Biomedical Engineering & Biotechnology, vol. 4, no. 3, pp. 1-6. https://doi.org/10.33552/ABBA.2020.04.000590
5. J. Desai, P. Moga, and R. Patwardhan. (2022). Design and Implementation of IOT Based Smart Library. International Research Journal of Innovations in En gineering and Technology (IRJIET), vol. 6, no. 1,pp. 34-38.
6. Barger, Y. Manevich, H. Meir, and Y. Tock. (2021, July). A Byzantine Fault- Tolerant Consensus Library for Hyperledger Fabric. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, pp. 1- 9. https://doi.org/10.1109/ICBC51069.2021.9461142.
7. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, and C. Murthy. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, pp. 1-15. https://doi.org/10.1145/3190508.3190538.
8. R. S. S. Kumar and S. K. Singh. (2024, June). a library management sytem under Blockchain Technology. IEEE Access,vol.12,pp.45892-45901. https://doi.org/10.1109/ACCESS.2024.3401234.
9. M. A. M. H. Al-Maktoumi. (2025, August). A Survey on Blockchain Applications in Education: Opportunities and Challenges. IEEE Transac tions on Learning Technologies, vol. 18, pp. 123-135.
10. K. A. A. Kumar and S. S. Rani. (2022, October) Securing E-Library Sys Tem With Bimodal Biometric Technique, vol.39, no.5, pp.1567- 1575. https://doi.org/10.18280/ts.390512.
11. T. N. R. K. M. N. A. M. Z. A. Abd Aziz. (2023, January). RFID Based Automated Library Management System. International Journal for Researchin Applied Science and Engineering Technology (IJRASET), vol. 11, no.1, pp. 123-128.