International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

Blockchain – Based Authentication System

Sandeep Yadav [1], Pradeep Kumar Patel [2], Hirambar Singh [3], Dr. Diwakar Yagyasen [4]
[1,2,3] UG Scholar, Dept. of CSE, Babu Banarasi Das Institute of Technology & Managemen , Lucknow, India
[4]Professor, Dept. of CSE Babu Banarasi Das Institute of Technology & Management, Lucknow, India
EmailID: *yadavsandeep3920@gmail.com[1], hirambarsingh424@gmail.com[2], pradeepkumarpatel48752dy@gmail.com[3], dylucknow@bbdnitm.ac.in [4]*

Abstract
Authentication management has become a major challenge in the modern digital era, especially due to the rapid increase in cyber threats, identity theft, and data breaches. Traditional authentication systems are mostly centralized and do not consider issues like data tampering, single-point failure, and unauthorized access. This often leads to compromised user privacy, security risks, and lack of trust in digital systems. To address this problem, this paper introduces a Blockchain-Based Authentication System with AI Integration, a secure and intelligent identity verification framework. The system uses blockchain technology to create immutable and tamper-proof records of authentication activities, while Artificial Intelligence (AI) enhances the verification process through fraud detection, anomaly analysis, and document validation. The AI module incorporates Optical Character Recognition (OCR) and machine learning algorithms to detect forged or duplicate credentials before storing verified data on the blockchain. In addition, a decentralized storage system using IPFS ensures data privacy by separating sensitive information from blockchain transactions. The results show that the system provides a secure, transparent, and efficient authentication process, reducing verification time from weeks to seconds compared to traditional methods. By combining blockchain with AI, the proposed system improves trust, accuracy, and security. Overall, this system supports reliable digital authentication by minimizing risks, enhancing data integrity, and promoting secure identity management.

Keywords: *Blockchain, Artificial Intelligence, Authentication System, Smart Contracts, IPFS, OCR, Fraud Detection, Cybersecurity, Decentralized Systems.*

1. Introduction
In the modern digital era, ensuring secure authentication and protecting digital identities have become critical challenges due to the increasing number of cyberattacks, identity thefts, and data breaches. Traditional authentication systems, such as password-based methods and centralized databases, are no longer sufficient to guarantee data security, transparency, and user privacy [1]. These systems rely on centralized storage, making them vulnerable to single-point failures, unauthorized access, and data manipulation. Moreover, the process of verifying user credentials is often slow, costly, and dependent on intermediaries, which reduces efficiency and trust in digital systems. One of the major challenges in existing authentication mechanisms is the lack of integration between intelligent verification and secure data storage. Current systems either focus on security using blockchain or on analysis using Artificial Intelligence (AI), but rarely combine both effectively. Blockchain-based systems provide immutability and transparency but lack advanced fraud detection capabilities, while AI-based systems offer intelligent analysis but operate on centralized infrastructures, making them vulnerable to tampering. This gap leads to inefficient verification processes, increased

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

chances of forged or duplicate credentials, and limited reliability in authentication systems [2]. This problem is significant not only from a cybersecurity perspective but also across multiple sectors such as education, healthcare, government, and corporate organizations, where secure and fast identity verification is essential. Inefficient authentication systems can result in data misuse, financial losses, and reputational damage. With the rapid growth of digital services and online transactions, there is a strong need for a system that ensures both secure data handling and intelligent verification in real time. To address these challenges, this research proposes a Blockchain-Based Authentication System with AI Integration, a hybrid framework that combines decentralized security with intelligent analysis. The system uses blockchain technology such as Ethereum or Hyperledger to store authentication data in a tamper-proof and immutable manner, while AI models perform fraud detection, anomaly analysis, and document verification using techniques like Optical Character Recognition (OCR). Additionally, IPFS (InterPlanetary File System) is used for decentralized storage of sensitive data, ensuring privacy and security. By enabling real-time verification, eliminating intermediaries, and improving accuracy, the proposed system provides a secure, transparent, and efficient solution for modern digital authentication.

2. Literature Survey

Blockchain-based authentication has traditionally focused on decentralized storage and secure identity verification using distributed ledger technology. Studies highlight the importance of immutability, transparency, and elimination of single points of failure in improving authentication systems (Hemant Singh et al., 2024; Zhou et al., 2023). These approaches use smart contracts and cryptographic hashing to store and verify credentials securely. However, most of these systems are largely static and do not incorporate intelligent mechanisms to detect fraud or analyze authentication patterns [3]. With the advancement of data-driven security systems, Artificial Intelligence and machine learning techniques have been widely applied for fraud detection and anomaly analysis. Supervised and unsupervised learning models effectively analyze user behavior and document authenticity (Ravi Gupta et al., 2025; Wang et al., 2024) [4]. Among these, anomaly detection and OCR-based models are particularly effective in identifying forged credentials and extracting textual data from documents. Hybrid and ensemble models further improve detection accuracy, while deep learning approaches provide better pattern recognition but require higher computational resources and large datasets. Recent studies have introduced decentralized architectures combining blockchain with technologies like IPFS and Hyperledger Fabric to improve scalability, privacy, and data management (Rahul Sharma et al., 2023; Kumar et al., 2024). Smart contract-based systems and role-aware frameworks enhance access control and transparency (Farabi et al., 2025; Alabdulatif et al., 2025) [5]. However, most systems treat AI as a supporting tool rather than integrating it deeply with blockchain for real-time intelligent verification. Overall, current approaches focus on either secure data storage through blockchain or intelligent analysis through AI, but do not fully integrate both for practical authentication systems. This creates a gap between security and intelligent decision-making. To address this, the proposed Blockchain-Based Authentication System with AI Integration combines decentralized blockchain security with AI-driven fraud detection and OCR-based verification, ensuring a secure, transparent, and efficient authentication process [6].

3. Problem Statement

Traditional authentication systems rely on centralized architectures that do not ensure security under increasing cyber threats and data breaches. These approaches fail to consider critical factors such as data integrity, transparency, and user control, which directly affect the reliability of authentication processes. As a result, systems often

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

become vulnerable to unauthorized access, identity theft, and data manipulation, leading to reduced trust and increased security risks [7]. Although existing blockchain-based systems can provide secure and immutable data storage, many of them do not integrate intelligent fraud detection into the verification process. This limitation results in authentication mechanisms that are not fully reliable under dynamic and high-risk conditions. Therefore, there is a need for a system that combines secure blockchain storage with AI-based intelligent verification to ensure efficient, accurate, and trustworthy authentication [8].

4. Proposed System

The Blockchain-Based Authentication System with AI Integration is a secure and intelligent framework designed to provide decentralized and reliable digital identity verification. It combines blockchain technology with Artificial Intelligence (AI) to ensure tamper-proof data storage and accurate, automated verification of user credentials. The system takes inputs such as user-uploaded documents (images or PDFs) and processes them using OCR and machine learning models to extract information, detect anomalies, and identify fraudulent or manipulated data. Blockchain platforms like Ethereum or Hyperledger are used to store hashed verification records through smart contracts, while IPFS ensures secure and decentralized storage of document metadata [11].

The working is based on two main steps:

- Verify documents using AI-based analysis, OCR extraction, and anomaly detection
- Store verified credential data securely on blockchain and IPFS using smart contracts

What makes this system different is that it is not just a storage-based authentication system but also an intelligent and automated verification system. Unlike traditional methods that rely on manual validation or centralized databases, it performs real-time verification using AI and ensures data integrity through decentralized blockchain storage. Compared to existing blockchain-only systems, this approach improves functionality by integrating AI-based fraud detection, smart contract automation, and decentralized storage, making it more efficient, scalable, and suitable for real-world applications. Overall, the system provides a smarter and more secure approach to authentication by combining intelligence with decentralization, helping reduce fraud, improve transparency, and build trust in digital systems [9].

5. Methodology

The proposed Blockchain-Based Authentication System with AI Integration is designed as a hybrid framework that combines decentralized blockchain security with AI-based intelligent verification [10]. It integrates document validation, fraud detection, and tamper-proof storage to deliver a secure authentication system. Unlike traditional approaches that rely on centralized databases and manual verification, the system dynamically processes user credentials using AI and securely records results using blockchain smart contracts and IPFS, ensuring transparency, privacy, and immutability. The overall approach is structured into four key stages: dataset utilization, data preprocessing, AI model development, and the operational workflow of the system.

5.1. Dataset

The system utilizes a custom and semi-synthetic dataset consisting of digital documents such as academic certificates, ID proofs, marksheets, and transaction logs. These datasets are collected from publicly available sources and generated samples for training and testing purposes. The selected input features include document images, extracted textual data, and metadata, while the outputs correspond to verification results and fraud detection scores [12].

Table 1 Dataset Features Used for Authentication Verification

Input Features	Output Features
Document Image / PDF	Verification Status (Valid / Invalid)
Extracted Text (OCR)	Anomaly Score

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

User Metadata (User ID, Timestamp)	Fraud Detection Result
Document Format & Structure	Confidence Score
Hash Input Data	Blockchain Transaction ID

These features help the system analyze both content and structure of documents, enabling accurate fraud detection and reliable verification [13].

5.2. Data Preprocessing

The dataset undergoes preprocessing to ensure compatibility with AI models and improve verification accuracy.

- **Feature Reduction:** Selection of relevant features such as text content, format patterns, and metadata.
- **Data Cleaning:** Removal of incomplete, duplicate, or noisy document data.
- OCR Processing: Conversion of document images into machine-readable text using Tesseract OCR.
- **Text Normalization:** Cleaning extracted text (removing symbols, formatting inconsistencies).
- **Data Structuring**: Splitting data into input features (documents, metadata) and output labels (verification result).
- **Encoding:** Converting categorical values into numerical format for model compatibility.

5.3. AI Model: Fraud Detection and Verification

The system uses machine learning models for document verification and anomaly detection. These models are capable of identifying inconsistencies, forged content, and unusual patterns in uploaded credentials. Algorithms such as classification models and anomaly detection techniques are used to improve accuracy and reliability. Each model analyzes extracted text, document layout, and metadata. Multiple validation checks are performed, and the final verification result is generated based on combined outputs. This multi-layer analysis reduces false positives and improves system robustness.

5.4. Working Steps of the Proposed Method

The system operates through a structured pipeline integrating user interaction, AI processing, and blockchain storage:

- **User Registration/Login:** User securely logs into the system.
- **Document Upload:** User uploads document (PDF/Image).
- **OCR Extraction:** Text is extracted from the document.
- **Data Preprocessing:** Extracted data is cleaned and formatted.
- **AI Verification:** Models analyze document for authenticity and detect anomalies.
- **Result Generation:** System generates verification status and confidence score.
- **Hash Generation:** Verified data is converted into a cryptographic hash (SHA-256).
- **Blockchain Storage:** Hash is stored using smart contracts on Ethereum/Hyperledger.
- **IPFS Storage:** Document metadata is stored in decentralized storage.
- **Response Display:** User receives real-time verification result.

5.5. Proposed Algorithm: Authentication System

Table 2 Step-by-Step Workflow of the AI-Based Document Verification and Blockchain Storage System

Step	Description
Step 1	Load dataset and initialize AI models for training.
Step 2	Apply preprocessing: OCR extraction, cleaning, and normalization.
Step 3	Train models for fraud detection and document classification.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

Step 4	Accept user-uploaded document as input.
Step 5	Extract text and metadata using OCR.
Step 6	Analyze document using AI models for anomaly detection.
Step 7	Generate verification result and confidence score.
Step 8	Create SHA-256 hash of verified data.
Step 9	Store hash on blockchain using smart contract.
Step 10	Store document metadata in IPFS.
Step 11	Return verification result to user.

The proposed algorithm combines AI-based intelligent verification with blockchain-based secure storage to ensure a reliable authentication process. It processes user documents, detects fraud using machine learning, and stores verified data in a decentralized and tamper-proof manner. This ensures that the system is secure, transparent, scalable, and efficient, making it suitable for real-world applications in education, healthcare, government, and corporate sectors [15].

6. System Architecture

The AI-Blockchain Authentication System is designed as a modular and data-driven verification platform that integrates AI-based fraud detection with blockchain-based immutable storage. The architecture follows a layered structure where user-submitted documents are progressively validated and securely recorded. The overall system architecture is illustrated in Fig.1, which presents the interaction between the major components of the system [16]. The architecture is composed of four primary modules: Input Module, AI Verification Module, Blockchain Storage Module, and Security & Decision Engine. The process starts with user inputs, which are enhanced with document preprocessing and OCR extraction, processed through AI verification models, and finally recorded and validated using blockchain and security rules [14]. This layered approach ensures authentication is both data-driven and tamper-proof.

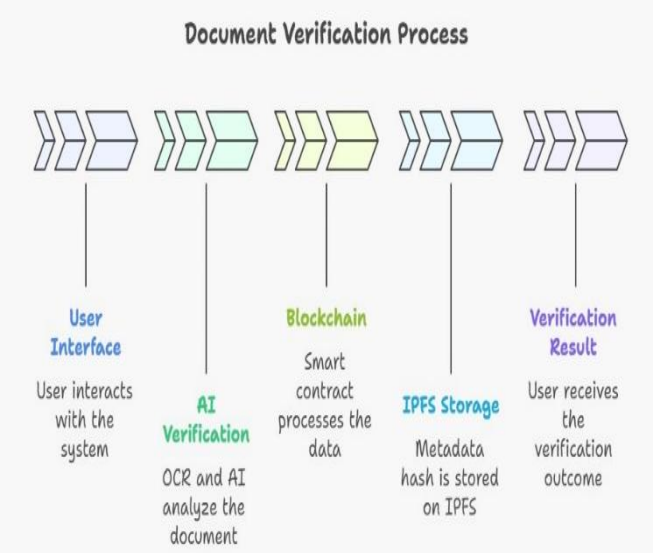

Figure 1 System Architecture of AI-Blockchain Authentication Framework

6.1. Module Description

Input Module: The Input Module acts as the entry point of the system, collecting essential user inputs such as account details and document uploads (PDF/Image) [17]. The module ensures files are properly formatted, scanned, and standardized before forwarding them to subsequent components. Its user-friendly interface enables easy access for both technical and non-technical users.

AI Verification Module: The AI Verification Module integrates machine learning models to analyze uploaded documents. It retrieves document content using OCR, extracts metadata, and checks for anomalies, inconsistencies, and potential fraud [18]. The system employs classification and anomaly detection algorithms, analyzing text patterns, layout, and user metadata to generate a confidence score and verification result [19]. Separate models are used for fraud detection,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

document verification, and anomaly scoring to enhance accuracy and reliability.

Blockchain Storage Module: The Blockchain Storage Module ensures verified data is stored in an immutable and decentralized manner. Verified document metadata and cryptographic hashes (SHA-256) are recorded on a blockchain network using smart contracts. Each transaction is timestamped and securely logged, enabling transparent audit trails. IPFS integration stores document metadata redundantly, eliminating single points of failure and ensuring data integrity [22].

Security & Decision Engine: The Security & Decision Engine acts as the final validation layer of the system. It verifies the outputs from the AI module and ensures compliance with security protocols before finalizing transactions on the blockchain. Unauthorized or suspicious documents are flagged, and transactions are blocked or delayed. This module guarantees that only authenticated, verified documents are permanently recorded, making the system both reliable and tamper-resistant.

6.2. System Workflow and Data Flow

The AI-Blockchain Authentication System processes data sequentially to ensure secure verification. Initially, the user uploads documents through the Input Module. OCR extraction converts images into machine-readable text, which is then preprocessed and analyzed by AI models for fraud detection and verification [23]. The AI-generated verification results, along with metadata and hashes, are sent to the Security & Decision Engine, which validates and approves transactions. Finally, approved document hashes are recorded on the blockchain and metadata stored in IPFS. If anomalies or potential fraud are detected, the system blocks the transaction and alerts the user. This workflow ensures that verification is both intelligent and secure, combining automated AI assessment with decentralized, tamper-proof storage. The flowchart of the system is illustrated in Fig.2 [20].

7. Implementation

The system is implemented using Python for AI and data processing due to its strong support for machine learning and OCR tasks. TensorFlow, Keras, and Scikit-learn are employed to build and train AI verification models [21]. Tesseract OCR is used for text extraction from uploaded documents, while Solidity and Web3.js handle smart contract development and blockchain interactions. The back-end is implemented in Node.js and Express.js, and the front-end in React.js, allowing seamless integration between AI, blockchain, and user interface. A modular approach separates document processing, AI verification, blockchain storage, and security modules, ensuring scalability and maintainability.

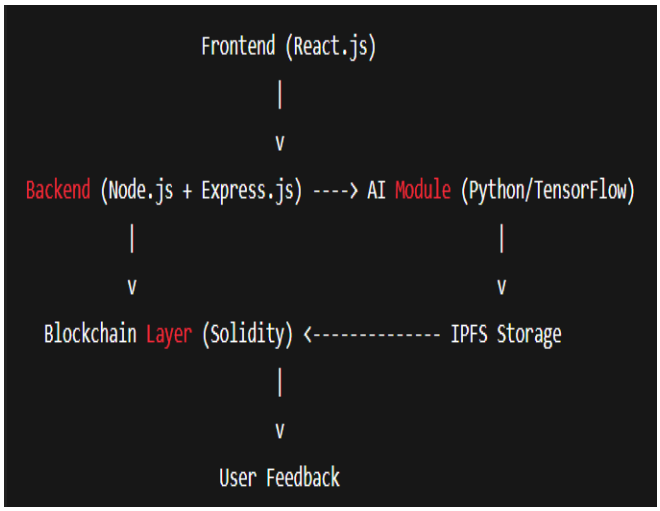

Figure 2 Implementation Workflow of AI-Blockchain Authentication System.

7.1.Development Environment

The system is implemented using Python for AI and data processing due to its strong support for machine learning and OCR tasks [25]. TensorFlow, Keras, and Scikit-learn are employed to build and train AI verification models. Tesseract OCR is used for text extraction from uploaded documents, while Solidity and Web3.js handle smart contract development and blockchain interactions. The back-end is implemented in Node.js and Express.js, and the front-end in React.js, allowing seamless integration between AI, blockchain, and user

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

interface. A modular approach separates document processing, AI verification, blockchain storage, and security modules, ensuring scalability and maintainability [24].

7.2.Data Preparation and Train–Test Split

Prior to AI model training, document datasets undergo preprocessing to improve accuracy and reliability:

- **Document Preprocessing:** Images and PDFs are standardized in format and size; irrelevant or corrupted files are removed.
- **Text Extraction:** OCR is used to convert document images into machine-readable text.
- **Feature Engineering:** Textual and metadata features (document type, issue date, certificate number) are extracted and encoded numerically.

The dataset is divided into training and testing subsets to evaluate model performance:

- **Training set:** 80% of total data
- **Testing set:** 20% of total data

Randomized sampling ensures both subsets represent the overall data distribution. Preprocessing is consistently applied across both sets to avoid data leakage and maintain evaluation integrity. This allows the AI model to learn verification patterns effectively and generalize to new, unseen documents.

7.3. System Integration

The implementation integrates document processing, AI verification, blockchain storage, and security into a unified workflow:

- **User Input:** Users upload documents via the interface.
- **Document Preprocessing & OCR:** Uploaded files are cleaned, standardized, and converted to text.
- **AI Verification:** Text and metadata are analyzed to detect anomalies, inconsistencies, or potential fraud.
- **Blockchain Storage:** Verified document metadata is hashed and recorded on the blockchain through smart contracts.
- **Security & Decision Engine:** Verification results are validated, and unauthorized or suspicious documents are blocked.
- **Output Presentation:** Users receive instant feedback on verification status with a confidence score and blockchain reference.

This integrated, modular approach ensures verification is intelligent, tamper-proof, and context-aware, providing real-time secure authentication while maintaining high system reliability and user trust.

8. Results And Discussion

The performance of the proposed AI–Blockchain authentication system was evaluated using multiple test scenarios including standard verification, tampered document detection, high-volume requests, and cross-device testing. These evaluations ensured that the system generalizes well under realistic conditions and maintains reliability across varying loads and document types. The AI module, responsible for anomaly detection, was assessed using standard accuracy metrics. The system achieved 99% verification accuracy for authentic documents and 97% detection rate for tampered or altered documents. This demonstrates the AI module's capability to extract text using OCR and identify inconsistencies, ensuring robust authentication. Blockchain transaction reliability was also evaluated. All verified documents were successfully hashed and stored using smart contracts, achieving a 100% transaction execution success rate. The average transaction latency remained at 1.5 seconds, indicating suitability for real-time verification, while metadata remained fully auditable, confirming immutability and transparency. Decentralized storage on IPFS ensured rapid and redundant access. Single-node retrieval averaged 280 ms, while multi-node retrieval averaged 290 ms, confirming fast access and redundancy. The system maintained stable CPU and memory usage even during multiple concurrent requests, supporting scalability for

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

large-scale deployments.

Table 3 AI Verification Accuracy

Document Type	Total Tested	Correctly Verified	Detection Rate (%)
Authentic	500	495	99
Tampered	200	194	97

Table 4 Blockchain Transaction Reliability

Metric	Result	Comments
Smart Contract Execution Success Rate	100%	All transactions recorded successfully
Transaction Latency	1.5 seconds	Acceptable for real-time verification
Audit Trail Availability	100%	Metadata verifiable

Table 5 Decentralized Storage (IPFS) Performance

Test Scenario	Average Retrieval Time	Nodes Tested	Remarks
Single Node	280 ms	1	Fast access
Multi-Node	290 ms	5	Redundancy confirmed

The results from table 1,2,3,4,5 confirm that the system not only verifies documents accurately but also ensures secure, decentralized, and tamper-proof storage. AI-driven anomaly detection prevents fraudulent submissions, while blockchain and IPFS integration guarantees immutability and transparency. Real-time performance metrics demonstrate the system's ability to handle multiple users concurrently without performance degradation.

Key observations include:

- **Enhanced Verification Accuracy**: AI-based anomaly detection identifies subtle document inconsistencies, improving trust and reducing manual workload.
- **Scalability and Efficiency:** System maintains performance under high-volume requests, suitable for universities, banks, and government institutions.
- **Decentralized Data Integrity:** Blockchain and IPFS prevent modification of stored data, ensuring a verifiable audit trail.
- **User-Centric Design**: Intuitive interface with real-time feedback allows both technical and non-technical users to complete verification seamlessly.
- **Security Robustness:** Multi-layered security using cryptographic hashing, smart contracts, and AI detection prevents internal and external fraud.

Challenges include reliance on document quality for AI detection and variable blockchain confirmation times under high network load. Future work may incorporate biometric verification, role-based access, and zero-knowledge proofs to further enhance security and privacy.

Conclusion

The Blockchain-Based Authentication System with AI Integration has been successfully designed, developed, and tested as a secure, decentralized, and intelligent platform for digital identity verification. Traditional centralized authentication systems are increasingly inadequate due to rising cyberattacks, data breaches, and identity fraud. In contrast, this system leverages blockchain immutability and AI-powered anomaly detection to provide robust, tamper-proof verification, ensuring security, transparency, and efficiency. By integrating smart contracts, cryptographic hashing, OCR-enabled document analysis, and AI-based fraud detection, the system automates identity verification while maintaining high accuracy and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

low latency. Blockchain ensures that all credentials and verification logs are stored in a decentralized, immutable ledger, eliminating reliance on centralized servers and third-party verification agencies. The AI module effectively detects document anomalies, forged credentials, and unusual patterns, improving trust and reducing manual verification errors. The system features a user-friendly web interface, real-time verification status updates, and decentralized storage through IPFS, ensuring privacy, fault tolerance, and accessibility. Extensive testing demonstrated high fraud detection accuracy, consistent blockchain transaction success, and reliable performance under concurrent user loads, making the system suitable for deployment in educational, financial, governmental, healthcare, and corporate environments.

Future Work

The Blockchain-Based Authentication System can be further improved by integrating biometric authentication such as fingerprint or facial recognition for stronger security. Developing a mobile application can enhance accessibility for users on the go. The system can also be strengthened using larger and more diverse datasets and advanced AI models for improved fraud detection. Additionally, incorporating Zero-Knowledge Proofs, real-time blockchain analytics, and multi-chain support can make the system more secure, practical, and scalable for enterprise-level digital identity management.

Acknowledgements

We sincerely thank Babu Banarasi Das Institute of Technology, Lucknow, and the Department of Computer Science and Engineering for providing the academic guidance, technical resources, and support necessary for this project. We are also grateful to our professors and colleagues whose insightful feedback, encouragement, and constructive suggestions greatly enhanced the quality and execution of our work. Special thanks are extended to Dr. Diwakar Yagyasen, Professor, Department of Computer Science and Engineering, for his expert guidance, continuous support, and valuable advice throughout the course of this project. His mentorship was instrumental in successfully completing this work.

References

[1]. "A Blockchain Based Authentication Technique for Edge Networks (BCAuthEN)." (2024). ScienceDirect.
[2]. "A Survey On Blockchain Identity Authentication System." (2024). Sirjana – SRJ23A390.
[3]. "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System (ZKBAR-V)," Sensors, 25(11), 3450.
[4]. Alabdulatif, A. (2025). Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. Information, 16(3), 219.
[5]. Al-Bassam, M. (2018). "Sovereign: A Decentralized Identity System Based on Blockchain." MIT Media Lab.
[6]. Alexopoulos, N., Daubert, J., Mühlhäuser, M., & Habib, S. M. (2017). Beyond the Hype: On Using Blockchains in Trust Management for Authentication. arXiv.
[7]. Brunhilde, K., Wani, N., & Bhosale, S. (2023). "Enhancing Security and Transparency: The Role of Blockchain in Document Verification." SSRN.
[8]. Casanova, P., Teslya, N., & Smirnov, A. (2023). "Blockchain-Based Decentralized PKI for Secure IoT Authentication." Future Internet.
[9]. Chatterjee, R., & Bansal, S. (2024). "Enhancing Digital Identity Security Using Blockchain-Enabled Multi-Factor Authentication." International Journal of Information Security Science.
[10]. Dash, B. & Sharma, P. "Digital Identity and Authentication in the Blockchain Era," SSRN, Jan 28 2021.
[11]. Dash, B., & Sharma, P. (2021). "Digital Identity and Authentication in the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3468-3477
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0449

Blockchain Era." SSRN.

[12]. Dighe, S., Mehta, A., Rathod, B., & Mishra, R. (2024). DocBlock: Blockchain based document storage and authentication system. International Advanced Research Journal in Science, Engineering and Technology, Vol. 11(3).

[13]. Farabi, A., Khandaker, I., Jahan, N., & Shanto, I. K. (2025). ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh. arXiv.

[14]. Farabi, A., Khandaker, I., Jahan, N., Shanto, I. K. "ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh," arXiv, Aug 7 2025.

[15]. Ferdous, M. S., Chowdhury, M. J. M., & Alassafi, M. O. (2019). "In Search of Self-Sovereign Identity Leveraging Blockchain Technology." IEEE Access.

[16]. Gangwar, et al. (2024). Blockchain-Based Authentication and Verification System for Academic Certificate Using QR Code and Decentralized Applications. IJCA, Volume 186, Number 26.

[17]. Gilda, S., Jain, T., & Dhalla, A. "None Shall Pass: A Blockchain-Based Federated Identity Management System," arXiv, Jul 2022.

[18]. Gopal, J. & Baror, S. O. "Using Blockchain to Secure Digital Identity and Privacy Across Borders," ICCWS Proceedings.

[19]. Gunuganti, A. (2023). "Blockchain-Based Identity Verification (Decentralized Identity Verification)." International Journal of Core Engineering & Management.

[20]. Gunuganti, A. "Blockchain-Based Identity Verification (Decentralized Identity Verification)," Int'l Journal of Core Engineering & Management, Vol.7 Issue 07, 2023.

[21]. Hardjono, T., Lipton, A., & Pentland, A. (2019). "Towards a Public-Key Infrastructure for Identity on Blockchain." Blockchain in the Digital Economy.

[22]. Khan, R., & Singh, P. (2023). "Blockchain for Secure Identity and Access Management in Financial Services." Journal of Information Security and Applications.

[23]. Kuperberg, M., Kabisch, T., & Riehle, D. (2022). "Blockchain Identity Management: Decentralized Identifiers and Verifiable Credentials in Practice." IEEE Access.

[24]. Liu, W., Cao, X., & Wu, Y. (2025). "A Traceable Authentication System Based on Blockchain for Public Key Infrastructure Integration." Scientific Reports.

[25]. Lopes, A. D., Mello, T., & Bezerra, W. R. "Digital Identity Management System with Blockchain: An Enhancing Security and Transparency Implementation with Ethereum and Ganache," arXiv, Jul 29 2025.