IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

SKY SHIELD A SKETCH-BASED DEFENSE SYSTEM AGAINST APPLICATION LAYER DDOS ATTACK

Mrs. R. Janaki, ME., Srikanth S, Krishnaraj K

Assistant Professor, CSE & Dhanalakshmi Srinivasan College of Engineering & Technology, India[1]

CSE (Cyber Security) & Dhanalakshmi Srinivasan College of Engineering & Technology, India[2]

CSE (Cyber Security) & Dhanalakshmi Srinivasan College of Engineering & Technology, India[3]

Abstract: The rapid growth of digital technologies, cloud computing, online learning platforms, and decentralized communication systems has increased the demand for secure academic credential management and intelligent cybersecurity solutions. Traditional credential verification systems mainly rely on centralized databases, which are vulnerable to data tampering, certificate forgery, unauthorized access, privacy breaches, and cyber attacks. To overcome these limitations, this paper proposes an AI-powered Blockchain Academic Validation Engine (BAVE-Chain) integrated with decentralized storage and intelligent cyber attack detection mechanisms.

The proposed system combines blockchain technology, smart contracts, InterPlanetary File System (IPFS), machine learning algorithms, and real-time monitoring techniques to provide secure credential verification and advanced cybersecurity protection. Blockchain technology ensures tamper-resistant storage of academic records and verification transactions, while IPFS provides decentralized and secure storage of certificates and supporting documents. Smart contracts automate verification and approval processes, improving transparency and reducing manual intervention.

The system also integrates machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and XGBoost for analyzing network traffic patterns and detecting malicious activities in real time. The proposed framework provides functionalities including student registration, certificate generation, decentralized credential storage, blockchain verification, traffic monitoring, alert generation, and dashboard visualization through Streamlit-based interfaces.

Experimental analysis and system testing demonstrate that the proposed framework effectively improves credential security, verification transparency, decentralized data management, and cyber attack detection accuracy. The integration of blockchain technology, artificial intelligence, and decentralized storage significantly reduces the risks of credential forgery, unauthorized access, and malicious network activities. Overall, the proposed BAVE-Chain framework offers a secure, scalable, intelligent, and reliable solution for modern academic credential validation and cybersecurity applications.

Keywords: Blockchain, Academic Credential Verification, BAVE-Chain, Smart Contracts, IPFS, Machine Learning, Cyber Attack Detection, Artificial Intelligence, Decentralized Storage, Network Security, Credential Validation, Random Forest, SVM, XGBoost, Cybersecurity.

INTRODUCTION

The rapid advancement of digital technologies, cloud computing, online education platforms, and decentralized communication systems has significantly transformed the management and sharing of academic credentials and sensitive information. Educational institutions, organizations, and employers increasingly rely on digital certificates and online verification systems for validating academic achievements and professional qualifications. However, traditional credential verification systems are mainly centralized, making them vulnerable to data tampering, certificate forgery, unauthorized access, privacy breaches, and cyber attacks. The increasing number of cyber threats and fraudulent credential activities has created a strong demand for secure, transparent, and intelligent verification mechanisms.

Blockchain technology has emerged as an effective solution for secure and tamper-resistant data management due to its decentralized architecture, transparency, immutability, and cryptographic security features. Blockchain enables secure storage of transaction records and prevents unauthorized modification of stored information. Smart contracts further enhance blockchain systems by automating verification and approval processes without requiring third-party

DOI: 10.17148/IJARCCE.2026.155151

intervention. Similarly, the InterPlanetary File System (IPFS) provides decentralized storage capabilities for securely managing large digital files such as academic certificates and supporting documents while generating unique cryptographic hashes for integrity verification.

Along with secure credential management, modern digital systems also require strong cybersecurity mechanisms to detect and prevent malicious activities in real time. Cyber attacks such as DDoS attacks, unauthorized access attempts, malicious traffic generation, and application-layer attacks can compromise system security and data integrity. Artificial Intelligence and Machine Learning technologies provide intelligent approaches for analyzing network behavior, identifying suspicious activities, and detecting cyber threats automatically. Machine learning algorithms such as Random Forest, Support Vector Machine (SVM), and XGBoost are widely used for traffic classification, anomaly detection, and real-time attack prediction.

To address these challenges, this paper proposes an AI-powered Blockchain Academic Validation Engine (BAVE-Chain) integrated with decentralized storage, smart contracts, machine learning-based cyber attack detection, and real-time monitoring mechanisms. The proposed framework combines blockchain technology, IPFS storage, intelligent verification, and cybersecurity monitoring into a unified secure system. The system provides functionalities such as student registration, credential generation, blockchain verification, decentralized file storage, attack detection, alert generation, and dashboard visualization.

The proposed system aims to improve credential authenticity, prevent certificate forgery, enhance transparency, provide decentralized data management, and strengthen cybersecurity protection against modern cyber threats. Experimental analysis and testing demonstrate that the proposed framework offers secure, scalable, reliable, and intelligent credential verification and cyber attack detection capabilities suitable for educational institutions, organizations, and modern digital infrastructures.

LITRETURE REVIEW

Satoshi Nakamoto (2008) introduced blockchain technology as a decentralized and tamper-resistant transaction management system through Bitcoin. The study demonstrated how distributed ledger technology can ensure transparency, immutability, and secure transaction validation without relying on centralized authorities. Although the work mainly focused on cryptocurrency transactions, the fundamental concepts of decentralized verification and cryptographic security laid the foundation for blockchain-based academic credential management systems.

Gavin Wood (2014) proposed Ethereum as a decentralized platform supporting smart contracts and programmable blockchain applications. The study highlighted the capability of smart contracts to automate verification, authorization, and transaction execution processes without third-party intervention. However, the research mainly concentrated on decentralized financial applications and did not specifically address academic credential verification or cybersecurity monitoring.

Juan Benet (2014) introduced the InterPlanetary File System (IPFS), a decentralized peer-to-peer storage mechanism designed for secure and distributed file management. The proposed architecture provided content-addressable storage using cryptographic hashes to improve file integrity and decentralization. While IPFS effectively supports distributed storage of digital documents, the framework alone does not provide intelligent verification or cyber threat protection mechanisms.

M. Swan (2015) discussed the broader applications of blockchain technology beyond cryptocurrency systems, including digital identity management, secure data sharing, and decentralized trust mechanisms. The research emphasized blockchain transparency and security advantages for organizational applications. However, the study lacked integration of artificial intelligence and real-time cyber attack detection capabilities within blockchain environments.

Cortes and Vapnik (1995) introduced the Support Vector Machine (SVM) algorithm for classification and pattern recognition tasks. SVM became widely adopted for network traffic analysis, anomaly detection, and cyber threat classification due to its strong predictive capability in high-dimensional datasets. However, standalone SVM models may face scalability limitations when processing large real-time network traffic environments.

Breiman (2001) proposed the Random Forest algorithm as an ensemble machine learning approach for classification and prediction tasks. Random Forest demonstrated high accuracy, robustness, and efficient handling of complex datasets in

DOI: 10.17148/IJARCCE.2026.155151

intrusion detection and cybersecurity applications. Nevertheless, the algorithm may require significant computational resources during large-scale deployment and real-time monitoring operations.

Chen and Guestrin (2016) developed the XGBoost algorithm as a scalable gradient boosting framework for efficient machine learning prediction. The model achieved high accuracy in anomaly detection, cyber attack classification, and traffic analysis applications. Although XGBoost improves prediction performance, the computational overhead and parameter optimization complexity remain significant challenges in real-time deployment.

Dorri, Kanhere, and Jurdak (2016) explored blockchain integration within Internet of Things (IoT) environments for secure decentralized communication and data protection. The study demonstrated how blockchain can improve authentication and data integrity in distributed systems. However, the proposed framework did not include decentralized academic credential management or intelligent machine learning-based attack detection.

Conti et al. (2018) presented a comprehensive survey on blockchain security and privacy issues, highlighting vulnerabilities such as unauthorized access, smart contract attacks, and scalability challenges. The research emphasized the importance of integrating advanced security mechanisms with blockchain systems to improve trust and resilience. However, the work did not propose a unified solution combining blockchain, decentralized storage, and artificial intelligence.

Stallings (2017) discussed network security essentials, cryptographic protocols, intrusion detection systems, and secure communication mechanisms. The research provided fundamental concepts for protecting modern digital infrastructures from malicious activities and unauthorized access. However, traditional security systems described in the study mainly relied on centralized architectures and lacked decentralized verification capabilities.

Recent studies on blockchain-based academic credential systems have focused on preventing certificate forgery, improving transparency, and automating credential validation. Many proposed systems successfully integrated blockchain and smart contracts for decentralized verification. However, several existing frameworks still suffer from scalability issues, limited interoperability, centralized storage dependencies, and lack of intelligent cybersecurity monitoring.

Similarly, modern cyber attack detection frameworks using machine learning algorithms have demonstrated high accuracy in traffic classification and anomaly detection. Despite these improvements, many systems fail to integrate decentralized storage, blockchain verification, and automated credential management within a unified secure architecture. Based on the analysis of existing literature, it is observed that there is a research gap in integrating blockchain technology, IPFS decentralized storage, smart contracts, machine learning-based cyber attack detection, and real-time monitoring into a single intelligent framework.

CONTRIBUTIONS OF THE PROJECT

1. The system integrates blockchain technology and smart contracts to provide tamper-resistant storage and automated verification processes.
2. The proposed framework uses IPFS decentralized storage for secure management of certificates and supporting documents.
3. Machine learning algorithms such as Random Forest, SVM, and XGBoost are implemented for intelligent cyber attack detection and traffic analysis.
4. The project introduces real-time monitoring and alert generation mechanisms for identifying suspicious network activities and malicious traffic behavior.
5. The framework improves transparency, trust, and security in academic credential management by eliminating centralized dependency.
6. The proposed system reduces certificate forgery, unauthorized modification, and data tampering through cryptographic verification mechanisms.
7. The system supports secure student registration, credential generation, decentralized verification, and blockchain transaction management.
8. The framework combines cybersecurity protection and credential verification within a unified intelligent architecture.
9. Experimental analysis demonstrates improved verification reliability, attack detection accuracy, scalability, and operational efficiency compared to traditional systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

METHODOLOGY

A. SYSTEM OVERVIEW

The proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) is designed to provide secure academic credential verification, decentralized storage, intelligent cyber attack detection, and real-time monitoring within a unified framework. The system integrates blockchain technology, smart contracts, IPFS decentralized storage, machine learning algorithms, and secure authentication mechanisms to improve transparency, data integrity, scalability, and cybersecurity protection.

The methodology consists of multiple phases including user registration, credential generation, blockchain transaction processing, decentralized file storage, machine learning-based attack detection, verification management, and real-time monitoring. The proposed architecture ensures that academic credentials are securely stored, verified, and protected from unauthorized modification and cyber threats.

B. SYSTEM PRELIMINARY

1. Blockchain Hash Generation

The blockchain hash generation process converts academic credential information into secure cryptographic hash values before blockchain storage.

[H = hash(D)]

Where:

□H□ → Generated hash value

□D□ → Credential data

This process ensures data integrity and tamper resistance within the blockchain network.

2. Smart Contract Verification

Smart contracts automatically validate credential transactions and verification requests.

[SC = Verify(T)]

Where:

□SC□ → Smart contract verification result

□T□ → Blockchain transaction

This mechanism improves automation, transparency, and trusted validation.

3. IPFS File Storage

The uploaded certificate file is stored within the IPFS decentralized storage network.

[CID = IPFS(File)]

Where:

□CID□ → Unique content identifier

□File□ → Uploaded certificate/document

This process provides decentralized and secure file management.

4. Machine Learning Classification

The machine learning module analyzes traffic behavior and classifies traffic as normal or malicious.

[f(x) = w^Tx + b]

Where:

□x□ → Input traffic features

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

□w□ → Weight vector

□b□ → Bias value

This classification supports intelligent cyber attack detection.

C. IMPLEMENTATION OF THE PROPOSED WORK

Step 1: User Registration

The user submits registration information such as student details, institution information, login credentials, and identification data through the system interface.

[U = {u_1, u_2, u_3, ..., u_n}]

Where:

□u_i□ → Individual user record

□n□ → Total number of users

The system validates user information before account creation.

Step 2: Credential Upload

Authorized institutions upload certificates and academic documents into the system.

[C = {c_1, c_2, c_3, ..., c_n}]

Where:

□c_i□ → Credential record

Uploaded files are forwarded for decentralized storage and blockchain processing.

Step 3: Data Preprocessing

The uploaded credential and traffic data are cleaned and normalized before analysis.

[D_p = Clean(D)]

This step improves consistency and machine learning prediction accuracy.

Step 4: Feature Extraction

Traffic and credential attributes are converted into feature vectors.

[x_i = (a_1, a_2, ..., a_m)]

Where:

□a_j□ → Feature attribute

□m□ → Number of features

This representation supports traffic analysis and attack detection.

Step 5: Blockchain Transaction Generation

Credential information and IPFS references are converted into blockchain transactions.

[T = {H, CID, Timestamp}]

Where:

□H□ → Credential hash

□CID□ → IPFS content identifier

The transaction is forwarded to the blockchain network.

Step 6: Smart Contract Execution

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155151

Smart contracts validate uploaded credential records automatically.

[Result = Execute(SC)]

If the validation is successful, the transaction is permanently added to the blockchain ledger.

Step 7: IPFS Decentralized Storage

The uploaded file is stored securely within the IPFS network.

[CID = SHA256(File)]

The generated CID is linked to the blockchain transaction for future retrieval.

Step 8: Traffic Monitoring

The system continuously monitors incoming network traffic and extracts behavioral patterns.

[Traffic = {r_1, r_2, r_3, ..., r_n}]

Where:

□r_i□ → Individual request record

This supports real-time attack analysis.

Step 9: Machine Learning Prediction

The machine learning model classifies traffic behavior using Random Forest, SVM, and XGBoost algorithms.

[y = \begin{cases} +1, & \text{Malicious Traffic} \ -1, & \text{Normal Traffic} \end{cases}]

The prediction result is stored for monitoring and analysis.

Step 10: Alert Generation

If suspicious traffic is detected, the system generates alerts and stores security logs.

[Alert = Detect(Attack)]

Administrators receive real-time notifications through the monitoring dashboard.

Step 11: Credential Verification

The verifier submits a credential validation request.

[Verify = Compare(H_1, H_2)]

Where:

□H_1□ → Submitted credential hash

□H_2□ → Blockchain stored hash

If both hashes match, the credential is verified successfully.

Step 12: Result Display

The system displays:

Verification status

Blockchain transaction details

Attack analysis results

Monitoring dashboard reports

Alert notifications

This improves transparency and operational efficiency.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

D. SECURITY AND PRIVACY MANAGEMENT

The proposed framework uses cryptographic hashing, blockchain verification, smart contracts, authentication mechanisms, and decentralized storage to protect academic credentials and operational data from unauthorized access and cyber threats. Machine learning algorithms provide intelligent threat analysis and improve attack detection accuracy within real-time monitoring environments.

E. SYSTEM ADVANTAGES

The methodology improves:

Credential authenticity

Decentralized verification

Cyber attack detection accuracy

Real-time monitoring efficiency

Tamper-resistant storage

Secure file management

Intelligent threat analysis

Transparency and trust management

Overall, the proposed methodology provides a scalable, secure, intelligent, and decentralized framework for academic credential validation and cybersecurity protection.

ALGORITHMIC STEPS

ALGORITHMIC STEPS
Algorithm 1: User Registration and Authentication
Input:
User registration details
Output:
Authenticated user account
Steps:
Step 1: Start the registration process
Step 2: Collect user information such as name, email, institution ID, and password
Step 3: Validate user input data
Step 4: Generate unique user identification number
Step 5: Encrypt login credentials using secure hashing
Step 6: Store user information in the database
Step 7: Verify login credentials during authentication
Step 8: Grant access to authorized users
Step 9: End the authentication process

Algorithm 2: Credential Upload and Blockchain Storage
Input:
Academic credential document
Output:

Blockchain transaction and IPFS hash
Steps:
Step 1: Start credential upload process
Step 2: Upload certificate/document into the system
Step 3: Generate cryptographic hash value for the file
Step 4: Store uploaded file in IPFS decentralized storage
Step 5: Generate IPFS content identifier (CID)
Step 6: Create blockchain transaction containing file hash and metadata

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

Step 7: Execute smart contract validation
Step 8: Store transaction in blockchain ledger
Step 9: Save transaction details in database
Step 10: End storage process

Algorithm 3: Machine Learning-Based Cyber Attack Detection
Input:
Network traffic data
Output:

Traffic classification result
Steps:
Step 1: Start traffic monitoring process
Step 2: Collect incoming network traffic requests
Step 3: Preprocess traffic dataset
Step 4: Extract traffic features and behavioral patterns
Step 5: Apply Random Forest, SVM, and XGBoost algorithms
Step 6: Analyze traffic behavior
Step 7: Classify traffic as normal or malicious
Step 8: Generate attack alerts for suspicious activities
Step 9: Store prediction and security logs in database
Step 10: End detection process

Algorithm 4: Smart Contract Verification
Input:
Credential verification request
Output:
Verification result
Steps:
Step 1: Start verification process
Step 2: Receive verification request from verifier or employer
Step 3: Retrieve blockchain transaction details
Step 4: Retrieve stored credential hash value
Step 5: Compare submitted credential hash with blockchain hash
Step 6: Execute smart contract verification
Step 7: Validate transaction authenticity
Step 8: Display verification result
Step 9: Store verification logs in database
Step 10: End verification process

Algorithm 5: Alert Generation and Monitoring
Input:
Attack prediction result
Output:
Security alert notification
Steps:
Step 1: Start monitoring process
Step 2: Analyze machine learning prediction result
Step 3: Detect abnormal traffic behavior
Step 4: Generate cyber attack alert
Step 5: Store attack logs in database
Step 6: Send alert notification to administrator
Step 7: Display monitoring analytics on dashboard
Step 8: Update real-time security reports
Step 9: End monitoring process

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

ARCHITECTURAL OVERVIEW

The proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) is designed using a multi-layered architecture that integrates blockchain technology, smart contracts, IPFS decentralized storage, machine learning algorithms, and real-time cybersecurity monitoring into a unified secure framework. The architecture is developed to provide secure academic credential verification, decentralized data management, intelligent cyber attack detection, and automated verification services.

The first layer of the architecture is the User Interaction Layer, which includes students, administrators, institutions, and verifiers interacting with the system through web and dashboard interfaces. This layer handles user registration, authentication, credential upload, verification requests, monitoring access, and report generation. The frontend interface is developed using Streamlit, HTML, CSS, and JavaScript to provide user-friendly interaction and real-time visualization.

The second layer is the Application Processing Layer, where backend processing and business logic are implemented using the Flask framework. This layer manages user authentication, credential processing, verification operations, blockchain communication, IPFS integration, machine learning prediction, and alert management. It acts as the central controller that coordinates communication between all system modules.

The third layer is the Blockchain and Smart Contract Layer, which ensures secure and tamper-resistant management of credential records and transaction data. Smart contracts automatically validate credential information and verification requests before storing transaction details in the blockchain ledger. Blockchain technology improves transparency, integrity, decentralization, and trust management within the system.

The fourth layer is the IPFS Decentralized Storage Layer, which securely stores uploaded certificates and supporting documents using distributed peer-to-peer storage mechanisms. Each uploaded file generates a unique cryptographic hash known as a Content Identifier (CID), which is linked with blockchain transactions for secure retrieval and integrity verification.

The fifth layer is the Machine Learning and Cybersecurity Layer, which continuously monitors network traffic and analyzes behavioral patterns using machine learning algorithms such as Random Forest, SVM, and XGBoost. This layer performs anomaly detection, cyber attack prediction, malicious traffic classification, and alert generation in real time to strengthen system security.

The final layer is the Database and Monitoring Layer, where transaction logs, credential records, verification details, security alerts, attack history, and monitoring reports are stored securely using SQLite database support. The monitoring dashboard provides real-time analytics, attack summaries, verification reports, and operational insights for administrators and authorized users.

Overall, the proposed architectural framework ensures secure credential verification, decentralized storage, intelligent cyber attack detection, transparency, scalability, automation, and real-time monitoring within a reliable and efficient cybersecurity environment.

4.1 Layer 1: Presentation Layer (Client Tier)

The Presentation Layer is the front-end interface of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain). This layer acts as the communication bridge between users and the internal system modules. It provides a user-friendly environment for students, administrators, institutions, verifiers, and security managers to access various functionalities of the system efficiently.

The presentation layer is developed using Streamlit, HTML, CSS, and JavaScript technologies to create responsive and interactive web interfaces. It handles user interactions such as registration, login authentication, credential upload, certificate verification requests, dashboard access, monitoring reports, and alert visualization. The interface is designed to simplify system usage while maintaining secure communication with backend modules.

Students can use this layer to register accounts, upload personal details, access certificates, and check verification status. Institutions and administrators can generate certificates, approve credential requests, monitor transactions, and manage blockchain verification operations. Verifiers and employers can submit credential verification requests and view validation results securely through the interface.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

The presentation layer also includes a real-time monitoring dashboard that displays network traffic analytics, cyber attack alerts, verification statistics, blockchain transaction details, and operational reports. Graphs, tables, and visualization components help administrators analyze system activities and monitor security events effectively.
Authentication and access control mechanisms are integrated into the presentation layer to ensure that only authorized users can access specific functionalities based on their roles and permissions. User inputs are validated before forwarding requests to backend processing modules, improving reliability and preventing unauthorized operations.
Overall, the presentation layer improves usability, accessibility, interaction efficiency, and visualization capabilities within the proposed blockchain-based credential verification and cybersecurity framework.

4.2 Layer 2: Application / API Layer (Backend Tier)

The Application and API Layer acts as the core processing and communication layer of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain). This layer manages business logic, request processing, data communication, blockchain interaction, machine learning operations, and integration between different modules within the system. It serves as the central controller that connects the presentation layer with backend services, databases, blockchain networks, and decentralized storage platforms.

The application layer is implemented using the Flask framework in Python, which provides secure and scalable backend processing capabilities. It handles operations such as user authentication, credential generation, blockchain transaction management, smart contract execution, IPFS communication, verification processing, machine learning prediction, traffic monitoring, and alert management.

The API layer enables secure communication between frontend interfaces, blockchain services, decentralized storage modules, and machine learning components through RESTful APIs. These APIs allow the system to exchange data efficiently between modules while maintaining interoperability and secure access control. API endpoints are used for functions such as user registration, login validation, certificate upload, credential verification, blockchain retrieval, IPFS file access, and attack prediction requests.

When a credential is uploaded, the application layer processes the file, generates cryptographic hashes, communicates with the IPFS storage network, and creates blockchain transactions through smart contracts. Similarly, verification requests are processed by retrieving blockchain records, validating hashes, and returning verification results to the frontend interface.

The machine learning module integrated within this layer analyzes network traffic features and predicts malicious or normal behavior using algorithms such as Random Forest, SVM, and XGBoost. The system automatically generates alerts and stores prediction results whenever suspicious activities are detected.

The application and API layer also manages security features such as encrypted communication, session handling, access control, input validation, and authentication mechanisms to prevent unauthorized access and protect sensitive information. Logging and monitoring functionalities are included to track system operations, user activities, and cyber attack events for auditing and analysis purposes.

Overall, the Application and API Layer provides secure communication, intelligent processing, decentralized integration, automation, scalability, and efficient coordination between all modules of the proposed blockchain-based credential verification and cybersecurity system.

4.3 Layer 3: Transaction & Concurrency Control Layer

The Transaction and Concurrency Control Layer is responsible for managing secure transaction processing, synchronization, consistency, and concurrent access operations within the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain). This layer ensures that multiple users and system modules can perform operations simultaneously without causing data conflicts, transaction failures, or integrity issues.

The transaction management mechanism handles operations such as credential uploads, blockchain transaction creation, smart contract execution, verification requests, IPFS storage communication, database updates, and security log management. Each transaction is processed in a controlled sequence to maintain consistency and prevent unauthorized modification of credential records and verification data.

Blockchain technology plays a major role in this layer by maintaining immutable and tamper-resistant transaction records through distributed ledger mechanisms. Every credential upload and verification operation generates a blockchain

DOI: 10.17148/IJARCCE.2026.155151

transaction containing cryptographic hashes, timestamps, transaction IDs, and verification metadata. Smart contracts automatically validate transactions before they are permanently added to the blockchain ledger.

Concurrency control mechanisms are implemented to manage simultaneous access by multiple users such as students, administrators, institutions, and verifiers. The layer prevents problems such as data inconsistency, duplicate transactions, race conditions, and unauthorized concurrent modifications. Database locking, transaction isolation, synchronization methods, and secure request handling techniques are used to maintain operational reliability.

The layer also supports rollback and recovery operations during transaction failures or unexpected system interruptions. If an operation fails during blockchain validation or database updates, the transaction is safely reverted to preserve system consistency and data integrity.

Transaction logs and audit records are continuously maintained to monitor all system activities, credential operations, verification events, and security-related actions. These logs improve accountability, transparency, and forensic analysis capabilities within the framework.

In addition, the concurrency control layer coordinates communication between blockchain networks, IPFS storage systems, databases, and machine learning modules to ensure smooth parallel execution of system processes. This improves system scalability and enables efficient handling of multiple verification and monitoring requests in real time.

Overall, the Transaction and Concurrency Control Layer enhances reliability, consistency, synchronization, secure transaction management, and operational stability within the proposed blockchain-based credential verification and cybersecurity framework.

4.4 Layer 4: Smart Contract Execution Layer

The Smart Contract Execution Layer is one of the core components of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain). This layer is responsible for automating credential verification, blockchain transaction validation, access control, and secure execution of decentralized operations within the blockchain network. Smart contracts eliminate the need for manual intervention and third-party verification by automatically enforcing predefined rules and validation conditions.

The smart contracts are implemented using blockchain technology and are deployed within the Ethereum network to manage credential-related operations securely. Whenever an institution uploads a certificate or academic document, the smart contract automatically verifies transaction details, validates file hashes, and stores immutable transaction records in the blockchain ledger. This ensures transparency, integrity, and tamper-resistant credential management.

The smart contract execution layer handles operations such as certificate generation, transaction authorization, credential approval, blockchain validation, user access control, verification requests, and audit management. Each transaction is assigned a unique transaction ID and timestamp, which improves traceability and accountability within the system.

When a verifier or employer submits a credential verification request, the smart contract retrieves the corresponding blockchain transaction and compares the submitted credential hash with the stored blockchain hash. If both values match, the credential is verified successfully; otherwise, the system rejects the verification request and identifies the credential as invalid or modified.

The smart contract layer also supports decentralized trust management by ensuring that all verification operations are executed transparently without depending on centralized authorities. Since blockchain records cannot be modified after validation, the system significantly reduces certificate forgery, unauthorized modification, and fraudulent verification attempts.

Security mechanisms such as cryptographic hashing, digital signatures, transaction validation, and permission-based access control are integrated into the smart contract execution process to strengthen operational security. The layer also interacts with the IPFS decentralized storage network to retrieve file references and maintain secure mapping between blockchain transactions and stored certificates.

Additionally, smart contracts generate event logs and transaction histories for auditing and monitoring purposes. These logs help administrators track system activities, verification operations, and transaction execution details efficiently.

Overall, the Smart Contract Execution Layer improves automation, transparency, reliability, decentralized verification, transaction integrity, and operational efficiency within the proposed blockchain-based credential verification and cybersecurity framework.

4.5 Layer 5: Event Processing and Notification Layer

The Event Processing and Notification Layer is an important component of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain). This layer is responsible for monitoring system activities, processing security events, analyzing verification operations, and generating real-time notifications for administrators and authorized

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

users. It improves operational awareness, system responsiveness, and cybersecurity management within the overall framework.

The layer continuously monitors activities such as credential uploads, blockchain transaction validation, smart contract execution, user authentication, verification requests, IPFS storage operations, and network traffic behavior. Whenever an important event or suspicious activity occurs, the system processes the event and triggers appropriate actions automatically.

Machine learning algorithms and monitoring mechanisms analyze traffic patterns and system behavior to identify abnormal activities, unauthorized access attempts, malicious traffic generation, and cyber attacks. If suspicious behavior is detected, the Event Processing Layer generates alerts and forwards notifications to administrators through the Streamlit dashboard and logging system.

The notification mechanism supports real-time alert generation for events such as failed login attempts, unauthorized verification requests, blockchain transaction failures, abnormal traffic behavior, and detected cyber attacks. Notifications may include warning messages, transaction details, attack summaries, timestamp information, and severity levels to assist administrators in quick decision-making and incident response.

The layer also maintains security logs and event history records within the database for auditing, analysis, and future investigation purposes. Event logs help track system operations, user activities, verification history, and attack detection results, improving transparency and accountability.

Overall, the Event Processing and Notification Layer enhances the reliability, security, monitoring capability, and operational efficiency of the proposed BAVE-Chain framework by providing intelligent event handling, automated alert generation, and real-time cybersecurity monitoring.

4.6 Layer 6: Data Persistence Layer

The Data Persistence Layer is responsible for securely storing, managing, retrieving, and maintaining all system data within the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain). This layer ensures reliable data storage, integrity, consistency, and long-term availability of credential records, blockchain transactions, verification details, security logs, monitoring reports, and operational information.

The layer uses SQLite database support for storing structured system data such as user registration details, login credentials, credential metadata, transaction histories, verification records, machine learning prediction results, attack logs, and monitoring information. Database tables are organized efficiently to support fast retrieval, secure access, and reliable transaction management.

Academic certificates and supporting documents are stored using the IPFS decentralized storage network, while blockchain transaction hashes and verification metadata are maintained within the blockchain ledger. The data persistence layer securely links blockchain records, IPFS content identifiers (CID), and database entries to maintain consistency across decentralized and centralized storage components.

Whenever a credential is uploaded, the system stores file metadata, transaction information, timestamps, verification status, and user-related details within the database. Simultaneously, the associated document is stored in IPFS, and its cryptographic hash is recorded on the blockchain. This combination improves tamper resistance, decentralization, and secure retrieval of academic records.

The data persistence layer also manages storage of machine learning datasets, traffic monitoring logs, attack detection reports, and system alerts generated during cybersecurity analysis. Historical traffic records and prediction outputs are maintained for future analysis, auditing, and performance evaluation purposes.

To ensure data integrity and reliability, the layer implements transaction management, concurrency control, backup mechanisms, recovery procedures, and secure access control techniques. Data encryption, authentication mechanisms, and role-based permissions are used to protect sensitive information from unauthorized access and malicious modification.

The layer supports efficient query processing, indexing, and data synchronization to improve system performance and scalability during multiple user operations and concurrent transaction processing. Audit logs and activity records are continuously maintained for accountability, transparency, and forensic investigation purposes.

In addition, the Data Persistence Layer coordinates communication between databases, blockchain networks, IPFS storage systems, machine learning modules, and monitoring dashboards to ensure smooth data flow and operational consistency throughout the framework.

Overall, the Data Persistence Layer improves secure data storage, decentralized file management, operational reliability, data integrity, transaction consistency, scalability, and long-term availability within the proposed blockchain-based credential verification and cybersecurity framework.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

4.7 Cross-Cutting Concerns

Cross cutting concerns are common functionalities and supporting mechanisms that affect multiple layers and modules within the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain). These concerns are integrated across the entire framework to improve security, reliability, scalability, monitoring, maintainability, and operational consistency. Unlike core business functionalities, cross cutting concerns operate throughout the system and support overall system performance and protection.

One of the major cross cutting concerns in the proposed framework is security management. Security mechanisms such as authentication, authorization, encrypted communication, blockchain verification, cryptographic hashing, digital signatures, and access control are implemented across all system layers to protect academic credentials and sensitive operational data from unauthorized access and malicious attacks.

Logging and auditing also act as important cross cutting concerns within the system. All user activities, blockchain transactions, credential operations, verification requests, machine learning predictions, and security events are continuously recorded in audit logs. These logs improve accountability, transparency, monitoring, and forensic investigation capabilities throughout the framework.

Exception handling and error management are integrated across the system to ensure stable operation during unexpected failures, invalid requests, transaction interruptions, or network communication errors. Proper error handling mechanisms improve reliability and reduce operational disruptions during credential verification and blockchain processing.

Real-time monitoring and alert generation are additional cross cutting concerns that support continuous observation of network traffic, user activities, transaction status, and system health. Machine learning algorithms analyze traffic behavior and generate alerts whenever suspicious activities or cyber attacks are detected, improving cybersecurity awareness and rapid response capability.

Performance optimization and scalability management are also implemented throughout the framework to support multiple user operations, concurrent transaction processing, blockchain communication, and decentralized storage access efficiently. Load balancing, optimized query processing, caching mechanisms, and transaction synchronization techniques help maintain system performance under high workloads.

Data integrity and consistency mechanisms ensure that credential records, blockchain transactions, IPFS file references, and database operations remain synchronized and protected against unauthorized modification. Transaction management and concurrency control techniques are integrated across multiple layers to maintain reliable data processing.

Interoperability and communication management are cross cutting concerns that enable secure interaction between frontend interfaces, backend services, blockchain networks, IPFS storage, machine learning modules, and databases through APIs and secure communication channels.

Overall, cross cutting concerns improve the overall quality, maintainability, security, transparency, scalability, and operational efficiency of the proposed blockchain-based credential verification and cybersecurity framework by supporting consistent functionality across all system components.

5.2 Frontend Implementation

The frontend implementation of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) is developed using Streamlit, HTML, CSS, and JavaScript technologies to provide an interactive, user-friendly, and responsive interface for academic credential management and cybersecurity monitoring. The frontend layer acts as the communication interface between users and the backend services, enabling secure access to system functionalities such as registration, credential upload, blockchain verification, attack monitoring, and dashboard visualization.

The Streamlit framework is used to design dynamic dashboards and real-time monitoring interfaces due to its simplicity, scalability, and efficient integration with Python-based machine learning and blockchain modules. HTML and CSS are used to enhance the visual appearance, layout structure, and responsiveness of the application, while JavaScript supports interactive functionalities and user actions.

The frontend system provides multiple interfaces for different user roles including students, administrators, institutions, and verifiers. The student interface allows users to register, upload certificates, view credential status, and request verification. The administrator dashboard provides functionalities for monitoring blockchain transactions, managing users, viewing security alerts, and analyzing network traffic behavior. The verifier interface allows organizations and employers to validate credentials through blockchain-based verification mechanisms.

Real-time visualization components are integrated into the frontend to display attack analytics, credential verification results, blockchain transaction details, security logs, and system performance graphs. Interactive charts and monitoring panels help administrators analyze malicious traffic patterns and suspicious activities efficiently.

Secure session handling and authentication mechanisms are implemented within the frontend to protect user access and maintain system confidentiality. The frontend also communicates with backend APIs for retrieving blockchain records, IPFS hashes, machine learning prediction results, and database information.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

5.10 Fault Tolerance and Reliability

The proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) is designed with strong fault tolerance and reliability mechanisms to ensure continuous system operation, secure credential verification, decentralized storage management, and real-time cyber attack monitoring even under abnormal conditions or partial system failures.

The blockchain architecture improves reliability by maintaining distributed copies of credential records and transaction data across multiple nodes. Since the blockchain ledger is decentralized and tamper-resistant, the failure of a single node does not affect the overall availability or integrity of stored academic credentials. Smart contracts also ensure automatic verification and transaction execution without relying on centralized servers, thereby reducing the risk of operational failure.

The IPFS decentralized storage mechanism further enhances fault tolerance by distributing certificate files and supporting documents across multiple storage nodes. Even fo ne storage node becomes unavailable, the files can still be retrieved securely from other available nodes using their unique cryptographic content identifiers (CID). This decentralized storage approach improves data availability, redundancy, and reliability compared to traditional centralized storage systems.

The machine learning-based cyber attack detection module continuously monitors network traffic and system behavior in real time. The framework can automatically detect suspicious activities, abnormal traffic patterns, and malicious requests while generating alerts and maintaining operational logs. This proactive monitoring capability helps prevent system downtime and improves overall cybersecurity resilience.

Database backup mechanisms, authentication controls, transaction validation, and logging systems are also implemented to maintain operational consistency and secure recovery during unexpected failures or cyber attacks. The system stores verification records, security logs, and monitoring reports securely for future analysis and recovery purposes.

The proposed framework also supports scalability and stable performance during multiple user requests and continuous verification operations. Load distribution mechanisms and decentralized processing reduce dependency on centralized infrastructure, thereby improving operational stability and system reliability.

Overall, the proposed BAVE-Chain framework provides high fault tolerance, reliable credential verification, decentralized data protection, secure storage availability, and resilient cybersecurity monitoring suitable for modern educational institutions and distributed digital environments.

EXPERIMENTAL SETUP

The experimental setup of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) is designed to evaluate the performance, security, scalability, and operational efficiency of the system in credential verification and cyber attack detection environments. The experiments are conducted using blockchain networks, decentralized storage mechanisms, machine learning algorithms, and real-time monitoring modules to analyze the effectiveness of the proposed framework under different operational conditions.

The implementation environment uses Python programming language for system development. Flask framework is used for backend processing and API management, while Streamlit is used for dashboard visualization and monitoring interfaces. SQLite database is implemented for storing user information, credential records, blockchain transaction details, attack logs, prediction results, and monitoring history. Ethereum blockchain is used for smart contract execution and decentralized transaction validation, while IPFS is used for decentralized storage of certificates and supporting documents.

The machine learning module is implemented using Scikit-learn and XGBoost libraries for network traffic analysis and cyber attack detection. Algorithms such as Random Forest, Support Vector Machine (SVM), and XGBoost are trained using network traffic datasets containing both normal and malicious traffic records. The datasets include traffic patterns related to DDoS attacks, unauthorized access attempts, abnormal request generation, and application-layer cyber attacks.

SYSTEM CONFIGURATION

Hardware Requirements

- Processor : Intel Core i5 or above

- RAM : 8 GB or higher

- Storage : 256 GB SSD

- Network : High-speed internet connectivity

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

Software Requirements

- Operating System : Windows 10/11 or Linux

- Programming Language : Python 3.x

- Frontend Framework : Streamlit

- Backend Framework : Flask

- Database : SQLite

- Blockchain Platform : Ethereum

- Decentralized Storage : IPFS

- Machine Learning Libraries : Scikit-learn, XGBoost, Pandas, NumPy

EXPERIMENTAL PROCEDURE

Step 1: User Registration and Authentication
Users and institutions register within the system using secure authentication credentials. The system validates login information and provides authorized access to the dashboard and credential management modules.
Step 2: Credential Upload and IPFS Storage
Academic certificates and supporting documents are uploaded into the system. The uploaded files are processed and stored within the IPFS decentralized storage network, generating unique content identifiers (CID) and cryptographic hash values.
Step 3: Blockchain Transaction Generation
Credential metadata and IPFS hash references are converted into blockchain transactions. Smart contracts automatically validate the transactions and store them securely within the Ethereum blockchain network.

Step 4: Credential Verification
Verification requests are submitted by authorized users or organizations. The system retrieves blockchain records, compares cryptographic hashes, and validates credential authenticity using smart contract verification mechanisms.

Step 5: Network Traffic Monitoring
The system continuously monitors network traffic and collects request behavior information such as source IP address, request frequency, traffic intervals, and communication patterns.

Step 6: Machine Learning Prediction
Extracted traffic features are analyzed using Random Forest, SVM, and XGBoost algorithms. The machine learning module classifies traffic as normal or malicious based on learned traffic behavior patterns.

Step 7: Alert Generation and Monitoring
If suspicious traffic or abnormal behavior is detected, the system automatically generates alerts and stores attack logs within the database. Real-time notifications and attack summaries are displayed through the monitoring dashboard.

PERFORMANCE EVALUATION METRICS

The proposed system is evaluated using the following performance metrics:

- Accuracy
- Precision
- Recall
- F1-Score
- Verification Efficiency
- Attack Detection Rate
- Transaction Validation Time
- Response Time
- Scalability Performance

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

These metrics are used to analyze credential verification reliability, blockchain performance, cyber attack detection capability, and operational efficiency.

RESULT OBSERVATION

The experimental analysis demonstrates that the proposed BAVE-Chain framework successfully provides secure credential verification, decentralized storage management, intelligent cyber attack detection, and real-time monitoring capabilities. The integration of blockchain technology, IPFS, smart contracts, and machine learning algorithms significantly improves transparency, security, verification accuracy, and protection against malicious activities compared to traditional centralized systems.
Overall, the experimental setup confirms that the proposed framework is scalable, reliable, intelligent, and suitable for modern academic credential verification and cybersecurity applications.

6.5 Performance Metrics
PERFORMANCE METRICS
The performance of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) is evaluated using several important performance metrics to analyze the effectiveness of credential verification, blockchain transaction validation, decentralized storage management, machine learning-based cyber attack detection, and real-time monitoring operations. These metrics help measure the accuracy, reliability, efficiency, scalability, and security capability of the proposed framework.

1. ACCURACY
Accuracy measures the overall correctness of credential verification and cyber attack detection performed by the system. It represents the ratio of correctly classified records to the total number of processed records.

[

Accuracy = \frac{TP + TN}{TP + TN + FP + FN}

]

Where:

- TP → True Positive

- TN → True Negative

- FP → False Positive

- FN → False Negative

Higher accuracy indicates better system reliability and prediction performance.

2. PRECISION

Precision measures the capability of the system to correctly identify genuine credentials and malicious traffic while minimizing false positive results.

[

Precision = \frac{TP}{TP + FP}

]

High precision improves trust and reduces unnecessary alert generation.

---

3. RECALL

Recall evaluates the ability of the system to detect all genuine verification records and malicious traffic activities successfully.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155151

[

Recall = \frac{TP}{TP + FN}

]

Higher recall ensures improved cyber attack detection capability and reduced attack leakage.

---

4. F1-SCORE

F1-Score provides a balanced evaluation of precision and recall performance.

[

F1\text{-}Score = \frac{2 \times Precision \times Recall}{Precision + Recall}

]

A higher F1-Score indicates balanced and consistent system performance.

---

5. VERIFICATION EFFICIENCY

Verification efficiency measures the effectiveness and success rate of blockchain transaction validation and credential verification operations.

[

Verification\ Efficiency = \frac{Successful\ Verifications}{Total\ Verification\ Requests} \times 100

]

This metric evaluates the operational reliability of smart contracts and decentralized verification mechanisms.

---

6. ATTACK DETECTION RATE

Attack Detection Rate measures the capability of the machine learning module to identify malicious traffic and cyber attacks correctly.

[

Detection\ Rate = \frac{Detected\ Attacks}{Total\ Attacks} \times 100

]

Higher detection rates improve cybersecurity protection and real-time threat management.

---

7. RESPONSE TIME

Response time measures the duration required for credential verification, blockchain validation, and attack detection processes.

[

Response\ Time = End\ Time - Start\ Time

]

Lower response time indicates faster system processing and improved operational efficiency.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

---

8. TRANSACTION VALIDATION TIME

Transaction validation time measures the duration required for blockchain transaction confirmation and smart contract execution.

[

Transaction\ Validation\ Time = Confirmation\ Time - Submission\ Time

]

This metric evaluates blockchain processing performance.

---

9. SCALABILITY PERFORMANCE

Scalability performance measures the ability of the system to handle increasing numbers of users, credential records, blockchain transactions, and network traffic requests.

[

Scalability = \frac{Processed\ Requests}{System\ Resources}

]

This metric evaluates the operational stability of the framework under large-scale workloads.

---

10. SECURITY RELIABILITY

Security reliability measures the effectiveness of authentication, blockchain integrity, decentralized storage protection, and cyber attack prevention mechanisms.

[

Security\ Reliability = \frac{Secure\ Operations}{Total\ Operations} \times 100

]

Higher reliability indicates stronger protection against unauthorized access and malicious activities.

---

11. STORAGE EFFICIENCY

Storage efficiency measures the capability of IPFS decentralized storage and database systems to manage credential records and transaction data efficiently.

[

Storage\ Efficiency = \frac{Stored\ Data}{Available\ Storage}

]

This metric evaluates decentralized storage optimization and resource utilization.

---

12. ALERT GENERATION ACCURACY

Alert generation accuracy measures the correctness of generated alerts during abnormal traffic detection and suspicious activity monitoring.

[

Alert\ Accuracy = \frac{Correct\ Alerts}{Total\ Alerts} \times 100

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155151

]

Higher alert accuracy reduces false alarms and improves monitoring efficiency.

Overall, these performance metrics confirm that the proposed BAVE-Chain framework provides secure credential verification, decentralized data management, intelligent cyber attack detection, efficient blockchain processing, and reliable real-time monitoring suitable for modern academic and cybersecurity applications.

DISCUSSION

The experimental analysis of the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) demonstrates that the integration of blockchain technology, decentralized storage, smart contracts, and machine learning algorithms significantly improves the security, transparency, reliability, and efficiency of academic credential verification and cybersecurity management systems. The obtained results confirm that the proposed framework successfully addresses many limitations present in traditional centralized verification systems.

The blockchain module provided tamper-resistant storage of credential records and verification transactions through decentralized ledger technology. Smart contracts automated the credential validation process and reduced manual intervention during transaction processing. This automation improved transparency, reduced verification delay, and minimized the possibility of unauthorized credential modification or certificate forgery.

The integration of IPFS decentralized storage improved secure management of certificates and supporting documents by generating unique cryptographic hashes for each uploaded file. The decentralized storage mechanism reduced dependency on centralized servers and improved data availability, integrity, and scalability. The generated IPFS content identifiers (CID) ensured secure retrieval and verification of stored files.

The machine learning-based cyber attack detection module demonstrated strong performance in identifying malicious traffic patterns, abnormal request behavior, and unauthorized access attempts. Algorithms such as Random Forest, Support Vector Machine (SVM), and XGBoost effectively classified network traffic as normal or malicious with high prediction accuracy. Real-time monitoring and alert generation mechanisms helped administrators respond quickly to detected cyber threats and suspicious activities.

Performance evaluation metrics such as Accuracy, Precision, Recall, and F1-Score confirmed that the proposed framework achieved better verification reliability and attack detection capability compared to traditional systems. The blockchain verification mechanism also improved transaction validation efficiency and operational transparency. Streamlit-based dashboard visualization provided effective monitoring of traffic analytics, attack summaries, verification logs, and blockchain transaction details.

Comparative analysis with existing systems showed that many traditional frameworks focus only on centralized credential verification or standalone cybersecurity monitoring. Existing systems often lack decentralized storage, intelligent threat analysis, automated verification, and real-time monitoring capabilities. In contrast, the proposed BAVE-Chain framework combines blockchain, IPFS, artificial intelligence, and cybersecurity monitoring into a unified secure architecture.

Although the proposed system achieved strong performance, certain limitations may arise during large-scale deployment. Blockchain transaction latency, computational overhead, storage complexity, and scalability challenges can affect system performance in high-volume environments. Additional optimization techniques and lightweight consensus mechanisms may be required to improve blockchain processing speed and resource utilization.

Future improvements can include deep learning-based attack detection, cloud-integrated blockchain deployment, distributed monitoring frameworks, multi-factor biometric authentication, and enterprise-level cybersecurity orchestration. Integration with advanced threat intelligence systems and SIEM platforms may further improve attack prediction and automated incident response capabilities.

Overall, the discussion confirms that the proposed AI-powered Blockchain Academic Validation Engine (BAVE-Chain) provides a secure, scalable, intelligent, and reliable solution for modern academic credential verification and cybersecurity protection while improving transparency, decentralization, and operational efficiency.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155151

REFERENCES

[1]. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[2]. M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.
[3]. N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, vol. 39, pp. 80–89, 2018.
[4]. Y. Zhang and J. Wen, "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things," Peer-to-Peer Networking and Applications, 2017.
a. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," arXiv preprint arXiv:1608.05187, 2016.
[5]. M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.
[6]. G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Project Yellow Paper, 2014.
[7]. Hyperledger Fabric Documentation, Linux Foundation, 2022.
[8]. Juan Benet, "IPFS – Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014.
a. M. Antonopoulos, Mastering Bitcoin, O'Reilly Media, 2017.
[9]. T. M. Mitchell, Machine Learning, McGraw-Hill Education, 1997.
[10]. C. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.
[11]. L. Breiman, "Random Forests," Machine Learning Journal, vol. 45, no. 1, pp. 5–32, 2001.
[12]. C. Cortes and V. Vapnik, "Support-Vector Networks," Machine Learning, vol. 20, pp. 273–297, 1995.
[13]. T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," Proceedings of the 22nd ACM SIGKDD Conference, 2016.
[14]. W. Stallings, Network Security Essentials, Pearson Education, 2017.
[15]. W. Stallings, Cryptography and Network Security, Pearson Education, 2018.
[16]. Bruce Schneier, Applied Cryptography, Wiley Publications, 2015.
[17]. RFC 791 – Internet Protocol Specification, IETF Standards Documentation.
[18]. RFC 793 – Transmission Control Protocol, IETF Standards Documentation.
[19]. OWASP Foundation, "OWASP Top 10 Web Application Security Risks," 2021.
[20]. NIST Cybersecurity Framework, National Institute of Standards and Technology, 2020.
[21]. M. Roesch, "Snort – Lightweight Intrusion Detection for Networks," USENIX Conference Proceedings, 1999.
[22]. V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks, 1999.
[23]. NIST Cybersecurity Framework, National Institute of Standards and Technology, 2020.
[24]. M. Roesch, "Snort – Lightweight Intrusion Detection for Networks," USENIX Conference Proceedings, 1999.

