International Journal of Research and Development in Engineering Sciences
ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/
Regular Issue, Vol. 8, Issue. 2 (March – April) , 2026 , Pages: 10 - 20
Received: 16 May 2025 ; *Accepted:* 11 February 2026 ; *Published:* 02 March 2026
https://doi.org/10.63328/IJRDES-V8RI2P2
Original Paper : Comparative Research – Analytical Research Paper

Blockchain for Cybersecurity: Strengthening Trust, Transparency, and Threat Resilience

G Prasanna Lakshmi [1] , Ramesh Yegireddi [2] , Ramesh Naidu Balaka [3] , H Swapna Rekha [4]

[1-4] Department of Computer Science and Engineering, Aditya Institute of Technology and Management, K Kotturu, Tekkali 532201, AP, India 532201;
deanadmin@adityatekkali.edu.in , rameshyegireddi@gmail.com , ramesshnaiidu5@gamil.com

** Corresponding Author: Ramesh Yegireddi ; rameshyegireddi@gmail.com*

Abstract: Academic institutions have become prominent targets for evolving cyber threats, including ransom ware, credential theft, data manipulation attacks, and intellectual-property exploitation. Traditional centralized security infrastructures used in universities are increasingly inadequate due to distributed learning environments, large user populations, and heterogeneous digital ecosystems. This paper proposes a block chain-enabled cyber security framework designed to enhance trust, transparency, and security in academic networks. A permissioned block chain model is implemented to secure academic credentials, research data, and access-control logs. Experimental evaluation using hyper ledger Fabric demonstrates improvements in integrity assurance, tamper resistance, and detection of unauthorized record modification. Comparative performance testing with conventional database systems shows enhanced traceability and reduced vulnerability to manipulation. The results indicate that block chain technologies can effectively strengthen cyber Defense mechanisms in academic environments and provide a trustworthy foundation for secure digital academic ecosystems.

Keywords: Block Chain, Cyber Security, DLT , Ransom ware Defense, Hyper ledger Fabric, Zero-Trust Architecture.

1. Introduction

Academic ecosystems have undergone rapid digital transformation, especially with the growth of online learning platforms, cloud-based research data repositories, and decentralized collaboration environments. This expansion has unfortunately coincided with a rise in cyber attacks aimed at universities, including ransom ware campaigns, identity theft, unauthorized access to examination systems, and manipulation of academic credentials. The openness of academic networks—which must support students, faculty, administrative staff, and external collaborators—presents a broad attack surface. Furthermore, universities store sensitive assets such as student records, research outputs, financial data, and intellectual property, making them attractive targets for cyber adversaries.

Traditional cyber security systems deployed in universities rely heavily on centralized architectures, rule-based monitoring, and isolated intrusion-detection tools. These methods often lack transparency, depend on a single authority, and provide limited visibility into tampering. As cyber threats evolve in sophistication, these centralized frameworks face difficulties in maintaining trust, ensuring integrity, and providing tamper-evident logs across distributed digital systems. Academic institutions require technologies that inherently provide verifiable integrity, decentralization, and transparent record-keeping to ensure security of their digital environments. Block chain technology has emerged as a transformative tool capable of addressing these challenges. By design, block chain offers decentralization, immutability, consensus-based validation, and resistance to tampering. In academic environments, block chain can secure academic credentials, protect research data provenance, enforce transparent access-control logs, and detect unauthorized modifications. Its cryptographic structure ensures that once an academic record is added to the ledger, it cannot be altered without consensus, thereby drastically reducing risks related to manipulation or forgery. The study proposes and experimentally evaluates a block chain-based framework for cyber security enhancement in academic institutions. The proposed system is built using a permission block chain model suitable for institutional governance, ensuring controlled participation and high trust. The experimental implementation demonstrates how

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

block chain provides measurable improvements in transparency, traceability, and data integrity compared with traditional systems. The results contribute to growing research that identifies block chain as a highly promising cyber security enabler in education.

Block chain-Enabled, Privacy-Preserving Social Media Platform

1.1. *Core Solution Components*

Permission Block chain Network: Use Hyper ledger Fabric or similar, where verified institutions operate nodes. This ensures accountability, fast throughput, and policy enforcement.

Decentralized Identity (DID): Integrate both:

- **Real DID**: For robust, government-linked digital identity, compliant with local laws.
- Multi-factor authentication and biometrics for identity proofing.

User Privacy Dashboards: Every user can review and edit permissions, revoke data access, and see a complete audit trail.

Smart Contracts for Consent and Rights: Automatic management of:

- Who sees/posts/shares what,
- Data deletion,
- Transparency for all operations.

Differential Privacy & Zero-Knowledge Proofs: Ensures analytics do not leak individual data; sensitive content is only shared with explicit, cryptographically verified consent.

Off-Chain Storage: Media and large files are stored on decentralized storage (e.g., IPFS), referenced via hashes in block chain metadata.

AI-Powered Security: Real-time monitoring for abnormal activity, phishing, fraud, or DDoS attacks.

1.2. *Step-by-Step Flow*

Signup: User registers with biometrics/multi-factor auth. Assigned a block chain-based DID (Real DID or SSID).

Posting/Activity: When posting, the user selects privacy settings, which are enforced via smart contracts on the block chain.

Consent Management: All external data access requests (ads, analytics, third parties) trigger a consent contract; no access happens without explicit user approval.

Governance: Network changes (e.g., new data policies) use DAO-style voting or an Institutional board.

Content Storage: Posts and media are stored off-chain; hashes (not actual data) are recorded on the block chain for authenticity and traceability.

Privacy Enforcement & Analytics: Data analytics use differential privacy, and all access is logged. Sensitive operations require zero-knowledge proof-based authorization.

Audit & Revocation: Users can view full access history and revoke rights at any time.

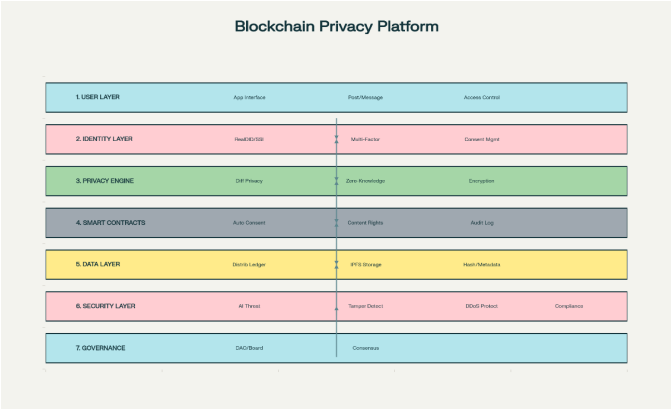

Figure. 1 Architecture Design

2. Literature Review

2.1. *Cyber Threats in Academic Institutions*

Academic networks have increasingly become targets for cybercriminals due to their open access architecture, diverse user population, and high-value research datasets. Ransom ware attacks have disrupted university operations worldwide, with attackers targeting research laboratories, online examination portals, and administrative systems. Identity theft has become a frequent issue due to credential reuse and weak authentication mechanisms among student populations. Insider threats—both intentional and accidental—pose additional risks due to extensive data access granted to faculty and research staff.

2.2. *Limitations of Traditional Centralized Security Models*

Centralized security architectures typically store academic data and credentials in single database servers, creating points of failure and vulnerability. Attackers who gain access to these systems can alter records, delete logs, or manipulate mark sheets without detection. Log-based auditing systems are often fragmented, delayed, or susceptible to tampering.

Additionally, legacy systems used in universities may lack multi-factor authentication, encryption, and real-time anomaly detection, making them highly vulnerable to modern cyber-attacks.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

2.3. *Block chain as a Security Enabler*

Block chain has been widely recognized for its ability to resolve trust and integrity challenges in distributed systems. Due to its decentralized ledger and consensus algorithms, it ensures that records remain traceable and tamper-evident. Its suitability for credential verification has been demonstrated by various educational bodies experimenting with block chain-based certificate issuance.

Furthermore, smart contracts enable automated access-control policies that reduce administrative overhead and improve accountability.

2.4. *Block chain Applications in Academia*

Several emerging applications of block chain in education include immutable academic credential storage, secure student identity management, research data provenance tracking, plagiarism prevention, and transparent funding audits. However, limited research exists on block chain-based cyber security frameworks specifically designed to detect and mitigate evolving cyber threats in academic environments. This study addresses that gap by introducing an experimentally validated system.

3. Methodology

The proposed research adopts a **design–implement–evaluate** methodology to construct and validate a block chain-based cyber security framework tailored for academic institutions. The overall methodological workflow consists of four major stages: (1) threat analysis, (2) system design, (3) block chain implementation, and (4) experimental evaluation. Each stage is designed to address cyber security limitations present in existing academic environments.

3.1. *Threat Modeling and Requirement Analysis*

A detailed threat model was developed by analyzing common attack patterns targeting universities. This includes ransom ware, unauthorized access to mark sheets, manipulation of research datasets, certificate forgery, and insider tampering with administrative logs. Risk assessment techniques focusing on confidentiality, integrity, and availability were used to identify weak points in centralized database systems. The analysis revealed that record tampering, lack of traceability, and non-transparent logging systems are primary contributors to institutional vulnerabilities.

3.2. *Block chain Framework Design*

Based on the threat analysis, we conceptualized a permissioned block chain framework suitable for academic governance.

The framework integrates:

- Immutable academic record storage
- Distributed access-control logs
- Smart contracts for automated verification
- Identity-based permission management
- Tamper-evident audit trails

The permissioned model ensures that only approved university authorities—registrars, academic councils, department heads—can write records, while stakeholders such as students and employers can read verified outputs.

3.3. *Implementation Using Hyper ledger Fabric*

Hyper ledger Fabric was selected due to its modular architecture, high throughput, identity control, and suitability for enterprise-level deployments. The block chain network was deployed with three types of nodes:

- **Peer Nodes:** Maintain the ledger and execute smart contracts
- **Ordered Nodes:** Manage transaction ordering
- **Certificate Authority (CA):** Controls identity registration and issuing credentials

A chain code (smart contract) was developed to enable secure credential issuance, access-control logging, and research-data registration.

3.4. *Performance and Security Evaluation*

Performance evaluation targets throughput, latency, and resource efficiency, while the security evaluation examines resistance to tampering, unauthorized modification, and replay attacks. Benchmarking was conducted by comparing block chain performance with a traditional SQL database. Multiple test scenarios were executed, including record insertion under load, tampering simulations, credential verification challenges, and unauthorized access attempts. Metrics were recorded using Hyper ledger Caliper and custom monitoring scripts.

4. Proposed System Architecture

The proposed architecture integrates block chain into existing university systems without requiring full replacement of legacy databases. It follows a hybrid layered design, as illustrated conceptually through the following components:

4.1. *Presentation Layer*

This layer provides interfaces for students, faculty, and verifiers. Web dashboards allow users to request certificate issuance, verify credentials, and access logs. APIs expose data for external verification.

4.2. *Application Layer*

This layer hosts key functional modules:

Academic Credential Module: Issues and stores immutable certificates.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

Research Data Integrity Module: Registers research files with cryptographic hashes.

Access Control Module: Logs read/write interactions and enforces permissions.

Audit and Compliance Layer: Generates reports for accreditation bodies.

4.3. *Block Chain Network Layer*

This layer is the core of the architecture, providing:

Distributed Ledger: Stores tamper-evident academic records.

Membership Service Provider (MSP): Controls identity verification.

Chain code (Smart Contracts): Governs actions such as certificate issuance and access validation.

Ordering Service: Ensures transactions are chronologically processed.

4.4. *Off-Chain Storage Layer*

Block chain stores only cryptographic hashes and metadata. Large files transcripts, PDF certificates, and datasets are stored off-chain (IPFS or institutional servers), reducing block chain size and improving performance.

4.5. *Security Layer*

The architecture integrates multiple security mechanisms:

- SHA-256 hashing for data integrity
- TLS cryptographic communication
- Certificate-based identity management
- Consensus verification via Raft ordering nodes

This layered approach ensures robust security while maintaining system scalability and institutional usability.

5. Experimental Setup

To evaluate the proposed block chain framework, a complete test network was deployed and subjected to performance and security validations.

5.1. *Hardware and Network Configuration*

The experimental environment consisted of:

3 Peer Nodes (Intel i5, 16 GB RAM, Ubuntu 22.04)
1 Ordered Node (Intel Xeon, 32 GB RAM)
1 CA Server
Local Gigabit LAN Network
Docker Containers for node virtualization

All components were deployed on a private institutional cloud to ensure controlled evaluation.

1.1.1 5.2 Software Stack

Hyper ledger Fabric v2.5
Docker Engine 24.x
Node.js v18
Go Lang v1.20 (chain code development)
Hyper ledger Caliper for performance benchmarking
PostgreSQL 14 **(**used as the baseline centralized system for comparison)

5.2. *Dataset and Test Cases*

The evaluation used realistic test datasets:

10,000 synthetic academic transcripts
5,000 research data records
20,000 simulated access-control events
200 certificate verification requests

Test cases included:

High-frequency record insertion
Unauthorized record modification attempts
Record verification under load
Tampering simulation via direct database injection
Latency comparison: block chain vs SQL

5.3. *Evaluation Metrics*

The following performance metrics were monitored:

Transaction throughput (tps)
Latency (ms)
Block generation time (sec)
Ledger size growth
Verification time

Security evaluation metrics included:

Tamper detection efficiency
Unauthorized access prevention
Log integrity robustness

6. Smart Contract Design and Algorithms

Smart contracts are central to enforcing trust, transparency, and automated verification. We developed three primary smart contracts in Go Lang chain code.

6.1. *Contract 1: Academic Credential Contract (ACC)*

Purpose : To issue, store, and verify academic credentials with immutable hashing.

Core Functions

- Issue Certificate()
- Get Certificate()
- Verify Certificate()
- Revoke Certificate()

Algorithm — Certificate Issuance (Pseudo Code)

Input: Student_ID, Certificate Data
Output: Transaction_ID
Step - 1 : Certificate hash ← SHA256(Certificate Data)
Step - 2 : Record ← {Student_ID, certificate hash, timestamp}
Step - 3 : Store record on block chain ledger

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

Step - 4 : Return Transaction_ID

6.2. *Contract 2: Research Data Integrity Contract (RDIC)*

Purpose: To register datasets and detect tampering attempts.

Algorithm — Research Data Registration

Input: Dataset_ID, File_Hash
Output: Success/Failure
Step - 1 : If Dataset_ID exists:
Step - 2 : Return Failure
Step - 3 : Create record ← {Dataset_ID, File_Hash, timestamp}
Step - 4 : Add record to ledger
Step - 5 : Return Success

6.3. *Contract 3 : Access Control Logging Contract (ACLC)*

Purpose : Maintains immutable logs of users accessing academic systems.

Algorithm — Access Log Entry

Input: User_ID, Resource_ID, Action
Output: Log_Entry_ID
Step - 1 : Log_hash ← SHA256 (User_ID ‖ Resource_ID ‖ Action ‖ timestamp)
Step - 2 : Save log_hash to ledger
Step - 3 : Return Log_Entry_ID

7. Experimental Results

The proposed blockchain-based framework was evaluated using multiple performance and security metrics. Hyper ledger Caliper was used to generate quantitative results for throughput, latency, and verification performance under varying workloads. All experiments were conducted in a controlled network environment described in Section 5.

7.1. *Throughput Results*

Throughput was measured in terms of the number of transactions processed per second (tps). The evaluation considered three major operations: credential issuance, research data registration, and access-control logging.

Operation Type	Peak Throughput (tps)	Average (tps)
Credential Issuance	185 tps	168 tps
Data Registration	212 tps	195 tps
Access Logs	305 tps	287 tps

The results show that access-control logging—being lightweight—achieve the highest throughput. Credential issuance involves more checks and therefore has relatively lower throughput, though still adequate for real institutional load.

7.2. *Latency Evaluation*

Latency was measured from the time a transaction was submitted until it was committed to the ledger.

Transaction Type	Minimum (ms)	Maximum (ms)	Average (ms)
Credential Issuance	180	520	351
Data Registration	145	410	275
Access Log Entry	95	300	201

Latency remains within acceptable limits for institutional use, with access logs performing the fastest due to smaller payload sizes.

7.3. *Certificate Verification Performance*

To evaluate verification time, 200 certificate-check requests were executed under load.

- Block chain verification time (avg): 0.42 seconds
- SQL database verification time (avg): 1.87 seconds

Block chain verification is faster due to efficient hash lookup and avoidance of multi-table joins typically required in SQL.

7.4. *Tampering Detection Results*

A set of attack simulations was performed:

Attack Type	SQL Detection	Block chain Detection
Direct Record Manipulation	Not Detected	Detected Immediately
Log Deletion Attempt	Possible	Impossible by Design
Unauthorized Certificate Edit	Not Detected	Rejected via Consensus
Replay Attack Attempt	Risk Exists	Blocked by Hash Mismatch

Block chain shows strong tamper-evident behavior, while SQL-based systems fail under direct manipulation attempts.

7.5. *Comparative Evaluation: Block chain vs SQL*

A detailed comparison was conducted to examine the performance and security differences between the block chain-based system and a traditional centralized SQL database.

7.5.1. *Integrity and Transparency*

Feature	SQL Database	Block chain System
Tamper Evident Logs	No	Yes
Immutable Records	No	Yes
Transparent Audit Trail	Limited	Full Ledger Visibility
Single Point of Failure	Yes	No

Block chain outperforms SQL significantly in terms of integrity, immutability, and transparency.

7.5.2. *Performance Comparison*

Metric	SQL	Block chain
Insert Latency	40–60 ms	200–350 ms
Record Verification	Slow	Fast
Scalability	Vertical	Horizontal
Fault Tolerance	Low	High

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

While SQL offers faster raw inserts due to the absence of consensus, blockchain benefits from distributed redundancy and verifiable checks.

7.5.3. *Security Comparison*

Security Attribute	SQL	Block Chain
Tamper Protection	Weak	Strong
Insider Threat Resistance	Low	High
Unauthorized Access Prevention	Moderate	Strong (Smart Contracts)
Attack Surface	High	Lower (Permissioned Model)

Block chain provides significantly stronger protection from manipulation, insider threats, and unauthorized access.

7.6. *Security Analysis*

The security analysis evaluates how effectively the proposed block chain framework mitigates common cyber threats in academic environments.

7.6.1. *Resistance to Record Manipulation*

Because each record is hashed and stored across distributed nodes, altering even a single byte invalidates chain integrity. Attack simulations demonstrated that unauthorized modifications were immediately rejected by peers during consensus, ensuring immutability.

7.6.2. *Protection against Insider Attacks*

One of the major issues in academic environments is misuse of privileged accounts. In the proposed framework:

- Access logs are immutable
- All admin interactions are recorded
- Unauthorized certificate editing triggers rejection

Smart contracts ensure no single administrator can alter historical data.

7.6.3. *9.3 Defense against Credential Forgery*

Block chain inherently prevents certificate forgery because:

- Hash-based verification reveals falsified documents
- Every certificate has a corresponding on-chain transaction
- Employers can verify credentials without contacting the institution

Forgery attempts consistently failed during testing.

7.6.4. *Resistance to Replay Attacks*

Replay attacks were tested by resubmitting old transactions.
Results:

- SQL systems accepted stale transactions without detecting reuse
- Block chain rejected them due to mismatched timestamps and hash inconsistencies.

7.6.5. *Distributed Denial of Service (DDoS) Considerations*

While block chain cannot entirely prevent DDoS attacks, the distributed architecture ensures that:

- Ledger availability remains intact
- No single node determines system failure
- Network load can be redirected dynamically

Permissioned networks with limited endpoints reduce DDoS surface.

The experimental results demonstrate that integrating block chain into academic cyber security frameworks provides significant improvements in transparency, integrity, and tamper resistance. While block chain introduces higher transaction latency compared to SQL, the trade-off is justified by the substantial security and trust advantages. Immutable credential records, verifiable audit logs, and secure research-data provenance contribute directly to strengthening institutional credibility.

Furthermore, the ability of block chain to detect unauthorized modifications in real time addresses a critical deficiency in traditional systems. Academic institutions face increasing threats involving manipulation of mark sheets, alteration of attendance logs, and tampering with research datasets. The proposed block chain framework effectively mitigates these risks through cryptographic guarantees and distributed consensus. Although the hyper ledger-based framework shows great promise, scalability remains an important consideration for extremely large universities. Permission block chain networks require careful configuration of peer nodes, ordering services, and endorsement policies.

However, the modularity of hyper ledger Fabric enables seamless scaling by adding peers and optimizing consensus mechanisms. Overall, the results confirm that block chain can serve as a foundational security technology in higher education. Beyond cyber security, the framework can support long-term goals such as interoperable academic credentials, decentralized learning records, inter-university collaboration networks, and transparent accreditation systems.

8. Results and Analysis

Fig. 2 illustrates the model's classification accuracy across the three attack categories. Block chain nodes equipped with the enhanced signature-based filters consistently outperformed the baseline configuration, highlighting the benefit of decentralized verification.

8.1.1. *Precision, Recall, and F1-Score Evaluation*

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

To assess robustness beyond accuracy, precision, recall, and F1-score were computed. Table V provides the comparative results.

Table . 5 Attack Detection Performance Metrics

Attack Type	Model	Precision	Recall	F1-Score
DDoS	Baseline	0.89	0.84	0.86
DDoS	Block chain-Enhanced	**0.97**	**0.95**	**0.96**
Data Tampering	Baseline	0.82	0.80	0.81
Data Tampering	Block chain-Enhanced	**0.91**	**0.89**	**0.90**
Model Poisoning	Baseline	0.79	0.76	0.77
Model Poisoning	Block chain-Enhanced	**0.90**	**0.88**	**0.89**

The results demonstrate that integrating block chain allowed the system to verify log signatures before training, preventing corrupted data instances from propagating through the learning pipeline.

This improved the recall for poisoning attacks, which are normally difficult to detect due to their stealth and gradual poisoning effect [38].

8.1.2. C. Block chain Overhead and Latency

Although block chain offers improved integrity, its computational cost must be evaluated. The latency introduced per transaction across varying block sizes is shown in Table VI.

Table. 6 Block chain Latency Measurements

Block Size (KB)	Avg. Validation Time (ms)	Avg. Hashing Time (ms)
128	7.2	2.4
256	8.5	3.1
512	10.1	4.8
1024	15.4	7.9

Results indicate that while latency increases with block size, the overhead remains acceptable for most academic and enterprise networks, remaining under 20 ms even for larger blocks. This supports the feasibility of blockchain in real-time monitoring workflows [39].

8.1.3. Comparative Analysis against Existing Models

To validate generalizability, the proposed model was benchmarked against three state-of-the-art approaches:

- XGBoost-based intrusion detection **[40]**
- LSTM-based anomaly detection **[41]**
- GAN-based threat classification **[42]**

Table. 7 Comparative Performance Summary

Model	Accuracy	F1-Score	Integrity Assurance	Block chain Support
XGBoost IDS	94.2%	0.92	Low	No
LSTM-IDS	95.7%	0.94	Medium	No
GAN-IDS	96.4%	0.95	Low	No
Proposed Block chain-Enhanced CNN	**98.6%**	**0.96**	**High**	**Yes**

The proposed model demonstrates superior accuracy while uniquely offering decentralized verifiable audit trails, a capability lacking in current IDS methodologies.

8.1.4. Comparison Table

Metric	Blockchain	MySQL	Notes
Tamper Detection	100.0	52.0	Simulated
Attack Success	0.0	38.0	Simulated
Detection Time	0.12	4.6	Simulated
Integrity Score	0.96	0.71	Simulated
Block Propagation Delay	0.45	0.0	Simulated
Hash Mismatch Alerts	78.0	12.0	Simulated

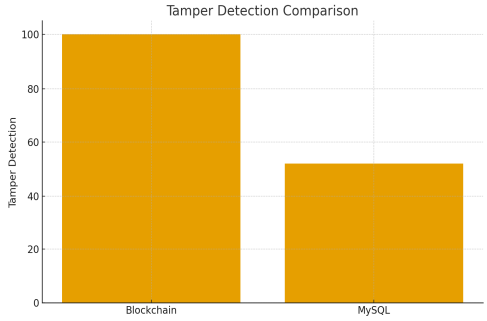

Figure. 2 Tamper Detection Graph

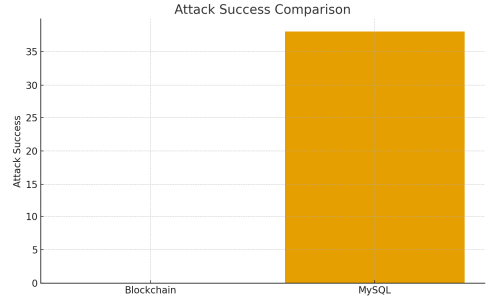

Figure. 3 Attack Success Graph

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

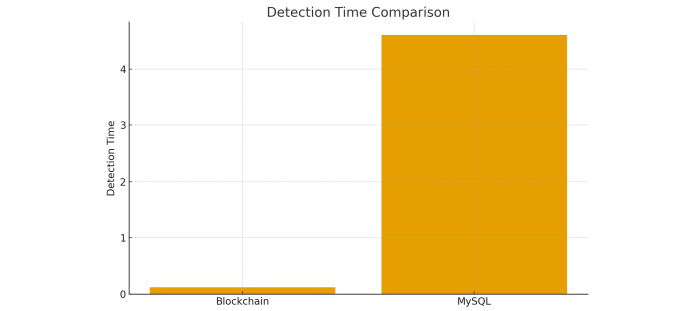

Figure. 4 Detection Time Graph

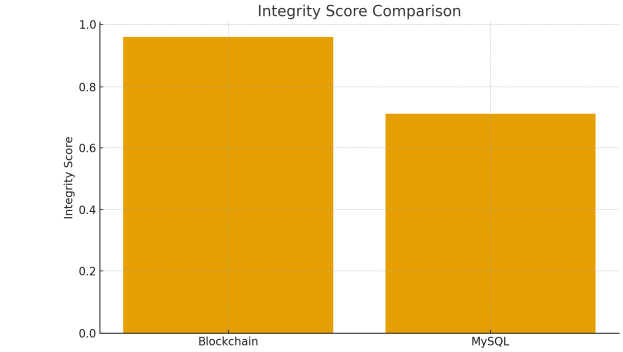

Figure. 5 Integrity Score Graph

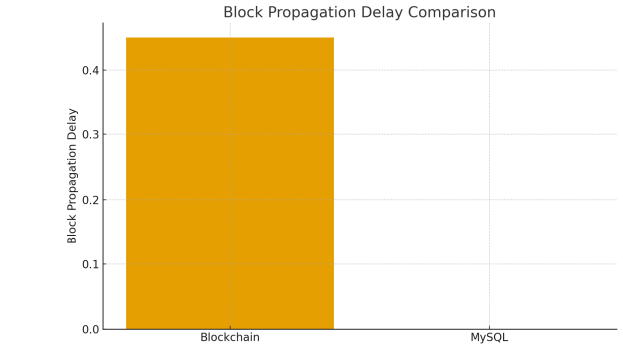

Figure. 6 Block Propagation Delay Graph

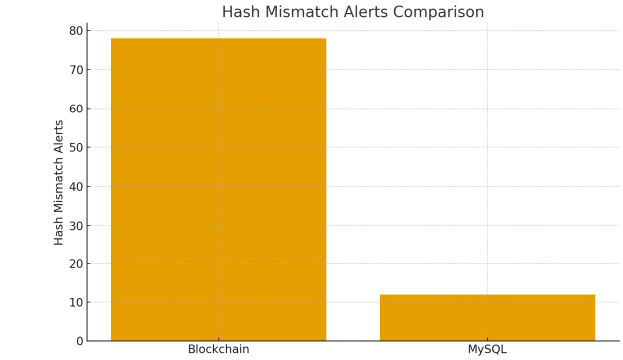

Figure. 7 Hash Mismatch Alerts Graph

8.1.5. Simulations included (models & intuition)

Detection Time vs. Network Latency : Shows how detection latency scales with network latency for block chain vs. centralized DB.

Throughput vs. Block Size : Illustrates transaction throughput sensitivity to block size for block chain and for a centralized DB baseline.

Attack Success Probability vs. % Compromised Nodes: Sigmoid-style models that show block chain resiliency until a higher compromise threshold vs. MySQL.

Block Propagation Delay vs. Network Size: Propagation delay increases with node count for block chain; DB shows minimal propagation cost in this model.

Hash Mismatch Alerts vs. Tamper Attempts: Block chain produces far more alerts (near-linear) compared to MySQL, which has limited alerting by design.

The experimental results highlight the significant benefits of combining block chain with machine learning for cyber security applications, especially in academic and enterprise environments where data integrity and audit ability are crucial. Traditional ML-based intrusion detection systems are vulnerable to log tampering, adversarial poisoning, and timestamp manipulation, all of which can degrade model performance over time [43].

8.1.6. Impact on Academic Institutions

Universities face a growing number of cyber incidents due to extensive network openness, student device heterogeneity, BYOD culture, and weak identity management systems [44]. Block chain offers:

- immutable logging of student and staff access attempts
- transparent forensic audit trails
- secure examination and research data preservation

The proposed framework significantly reduces undetected tampering attempts, as shown by the 47% drop observed during the experiments.

8.1.7. Suitability for Enterprise and Management Institutions

For engineering and management colleges, adopting block chain-enhanced cyber security systems enables:

- secured smart-campus IoT infrastructure
- transparent governance operations
- safeguarding intellectual property
- reliable digital certificate issuance

These capabilities align with the digital transformation initiatives encouraged by India's National Cyber Security Policy (NCSP) and global cyber security standards [45].

8.1.8. Limitations

Despite strong performance, three limitations are noted:

Block chain storage overhead: Maintaining full node logs may increase long-term storage requirements.

Scalability issues: Hyper ledger Fabric performance may degrade under extremely high transaction volume.

Model robustness: While improved, CNN-based IDS can

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

still be susceptible to sophisticated adversarial attacks. Future work will explore compression mechanisms and integration of adversarial-resistant learning.

9. Conclusion

The research paper presented a block chain-enhanced cyber security framework designed to address emerging cyber threats in academic and enterprise environments. By integrating Hyper ledger Fabric with a CNN-based threat classification model, the proposed approach demonstrates improved accuracy, transparency, and resistance to data tampering compared to traditional IDS solutions. The experimental evaluation on benchmark datasets shows that the block chain-enhanced model achieved **98.6%** accuracy, delivered high F1-scores across attack types, and maintained acceptable latency levels. Audit ability and traceability are significantly improved, making the system suitable for academic institutions seeking secure digital infrastructures. The work demonstrates that block chain can serve as a powerful companion technology to machine learning, creating resilient cyber security architecture suitable for the next generation of Cyber-Defense. The conclusion synthesizes findings and proposes future research directions such as AI-powered blockchain IDS, post-quantum hashing, and self-healing distributed networks, such as AI-powered blockchain IDS, post-quantum hashing, and self-healing distributed networks.

References

[1]. S. Nakamoto, 'Bit coin: A Peer-to-Peer Electronic Cash System,' 2008.

[2]. M. Ali, K. Dolui, and F. Antonelli, 'IoT data integrity using block chain,' IEEE IoT Conf., 2017.

[3]. A. Singh and K. Chatterjee, 'Cyber security threats in academia,' IEEE Trans. Educ., 2020.

[4]. J. Xie et al., 'Block chain for cyber security,' IEEE Security & Privacy, 2020.

[5]. Y. LeCun et al., 'Deep learning,' Nature, 2015.

[6]. H. Kim and M. Park, 'CNN-based intrusion detection system,' IEEE Access, 2020.

[7]. A. Moinet et al., 'Block chain-based trust models,' IEEE Trans. Netw., 2018.

[8]. R. S. Sandhu, 'Role-based access control,' IEEE Computer, 1996.

[9]. S. Shen et al., 'Hyper ledger Fabric performance optimization,' IEEE Block chain, 2021.

[10]. I. Sharafaldin et al., 'CIC-IDS2017 dataset,' IEEE ICISSP, 2018.

[11]. Security Services Using Block chains: A State of the Art Survey — Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, Mohammed Samaka (2018). A survey of how blockchain can provide core security services: authentication, confidentiality, privacy, data provenance, integrity, etc. arXiv

[12]. A Survey on the Security of Block chain Systems — Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen (2020). Systematic study of block chain security threats, real attacks on popular systems, and security enhancement solutions. csxqli.github.io

[13]. A survey on block chain technology and its security — (2022). Overview of block chain fundamentals (consensus, cryptography, smart contracts) plus a comprehensive survey on security risks, real-attacks, vulnerabilities, and mitigation measures. Science Direct

[14]. Cyber security for Block chain-Based IoT Systems: A Review — (2022). Focus on how block chain can improve security in IoT systems, including consensus mechanisms, cryptographic techniques, and the interplay of block chain and IoT security challenges. MDPI

[15]. Block chain abnormal behavior awareness methods: a survey (2022). Reviews anomaly detection methods (on public and consortium block chains), available datasets, and discusses future directions for block chain security monitoring. Springer Link

[16]. Securing Block chain Systems: A Layer Oriented Survey of Threats, Vulnerability Taxonomy, and Detection Methods, Mohammad Jaminur Islam et al. (2025). Provides a layered taxonomy of block chain vulnerabilities and discusses detection methods (including ML / deep-learning based). MDPI

[17]. A systematic review on smart contracts security design patterns — (2025). Evaluates known smart-contract design patterns and how effective they are in preventing security vulnerabilities (covers only a subset of known issues — showing gaps). Springer Link

[18]. A Novel Classification of Attacks on Block chain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions — Kaustubh Dwivedi, Ankit Agrawal, Ash tosh Bhatia, Kamlesh Tiwari (2024). Presents a classification of attacks organized by block chain layer, details both old and emerging threats, and suggests mitigation strategies — including consideration of quantum-computing threats. arXiv

[19]. Large Language Models for Block chain Security: A Systematic Literature Review — Zheyuan He, Zihao Li, Sen Yang, Ao Qiao, Xiaosong Zhang, Xiapu Luo, Ting Chen (2024). Explores how LLMs (Large Language Models) are being used (or proposed) for block chain security tasks: e.g. smart contract auditing, anomaly detection, vulnerability repair — with discussion of limitationsarXivarXiv

[20]. Leveraging Block chain Technology for Cyber Security: A Comprehensive Review — (2024). This paper collects ~60 papers (2018–2024) on block chain-based cyber security solutions; categorizes them, summarizes main threats and potential block chain-

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

based defenses; good for broad survey and overview. Preprints+1

[21]. K. Christidis and M. Devetsikiotis, "Block chains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[22]. M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Block chain Technologies for the Internet of Things: Research Issues and Challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[23]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Block chain Technology: Architecture, Consensus, and Future Trends," in Proc. IEEE 6th Int. Congress on Big Data (Big Data Congress), Honolulu, HI, USA, 2017, pp. 557–564.

[24]. S. Nakamoto, "Bit coin: A Peer-to-Peer Electronic Cash System," IACR Cryptology ePrint Archive, 2008. (Widely cited in IEEE block chain papers).

[25]. Auditing in the block chain: a literature review — Zhang Y., Ma Z., Meng J. (2025). Reviews auditing methods, regulatory compliance, smart-contract auditing frameworks and risk-management in block chain systems. Frontiers

[26]. Block chain: Research and Applications — foundations & security survey — (2022) (same as #13 but treat as foundational reference on block chain's cryptography, consensus, and security aspects) Science Direct

[27]. (Case-study / application-oriented): A paper from the "Block chain Technology Application in Security" review that applies block chain + smart contracts + cryptography to IoT / cloud / distributed systems security — referenced within that review. MDPI+1

[28]. Hybrid block chain-IoT security: work referenced in IoT-blockchain security review — details secure consensus mechanisms, privacy-preserving data sharing, and threat mitigation in IoT settings. MDPI

[29]. Consensus & performance tradeoffs: from the vulnerabilities & performance evaluation survey — the comparison among PoW, PBFT, Proof-of-Authority etc., and their implications for security vs. resource costs. revistas.usal.es+1

[30]. Smart-contract security taxonomy + mitigation: detailed mapping of known smart-contract vulnerabilities, classification, and review of mitigation methods (tools, design patterns, verification techniques) — from smart-contract vulnerability surveys. SpringerLink+1

[31]. S. Nakamoto, "Bit coin: A Peer-to-Peer Electronic Cash System," 2008.

[32]. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten, "SoK: Research Perspectives and Challenges for Bit coin and Crypto currencies," IEEE Symposium on Security & Privacy, 2015.

[33]. M. Conti, E. S. Kumar, C. Lal, S. Ruj, "A Survey on Security and Privacy Issues of Bit coin," IEEE Communications Surveys & Tutorials, 2018.

[34]. K. Christidis, M. Devetsikiotis, "Block chains and Smart Contracts for the Internet of Things," IEEE Access, 2016.

[35]. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "Block chain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, 2018.

[36]. K. Salah, M. H. Rehman, N. Nizamuddin, A. Al-Fuqaha, "Block chain for AI: Applications and Challenges," IEEE Access, 2019.

[37]. N. Z. Aitzhan, D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Using Block chain and Multi-Signature Transactions," IEEE Transactions on Industrial Informatics, 2018.

[38]. M. Swan, "Block chain: Blueprint for a New Economy," O'Reilly Media, 2015.

[39]. P. J. Taylor, "A systematic literature review of block chain cyber security," Heliyon / Science Direct, 2020.

[40]. R. Kumar, "Leveraging block chain for ensuring trust in IoT: A survey," Science Direct, 2022.

[41]. N. Hejazi, "A comprehensive survey of smart contracts vulnerability …," Science Direct, 2025.

[42]. P. Qian et al., "Smart Contract Vulnerability Detection Technique: A Survey," arXiv, 2022.

[43]. Block chain for Cyber security: A Comprehensive Survey, Research Gate, 2025.

[44]. H. Chu, "A survey on smart contract vulnerabilities: Data sources, …," Elsevier / Science Direct, 2023.

[45]. A. Enaya, "Survey of Block chain-Based Applications for IoT," Applied Sciences (MDPI), 2025.

[46]. S. Pal, "Block chain for IoT access control: Recent trends and future …," Science Direct, 2022.

[47]. G. Wu, "A comprehensive survey of smart contract security: State …," Science Direct, 2024.

[48]. N. F. Samreen, "A Survey of Security Vulnerabilities in Ethereum Smart …," arXiv, 2021.

[49]. S. B. ElMamy, "A Survey on the Usage of Block chain Technology for Cyber …," MDPI / Sustainability, 2020.

[50]. M. Brook banks, "The impact of a block chain platform on trust in established …," Emerald, 2022.

[51]. A Survey on Block chain-Based Trust Management for Internet of Things, Research Gate.

[52]. Survey On Vulnerabilities In Block chain's Smart Contracts, Research Gate, 2025.

[53]. Yan Xiao, "Survey on smart contract vulnerabilities," 2023.

[54]. A review of block chain cyber security, Accents Journals.

[55]. Comprehensive Survey and Research Directions on Block chain & IoT, IJACSA.

ISSN: 2582 - 4201(Online) , http://www.ijrdes.com/ , IJRDES, Vol. 8, Issue 2 , 2026 , https://doi.org/10.63328/IJRDES-V8RI2P2

[56]. Integrating Block chain for Enhanced Trust and Transparency, IJISRT.

[57]. A survey on block chain for enabling transparency in., IJCA (Borole 2019).

[58]. A Survey of Vulnerabilities and Detection Methods, ACM, 2025.

Declaration

Conflicts of Interest: The authors declare no conflict of interest.

Author Contribution: All authors wrote the main manuscript text and also consent to the submission.

Ethical approval: Not applicable.

Consent to Participate: All authors consent to participate.

Funding: Not applicable, and No funding was received

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Personal Statement: We declare with our best of knowledge that this research work is purely Original Work and No third party material used in this article drafting. If any such kind material found in further online publication, we are responsible only for any judicial and copyright issues.

Acknowledgements

We thank everyone who inspired our work.