



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





Decentralized Trust: Revolutionizing Data Security through Blockchain

Sripriya P¹, Dr. Seshu Babu Pulagara²

Research Scholar, Department of Computer Science, NITTTR, Chennai, India¹

Assistant Professor, Department of Computer Science & Engineering, NITTTR, Chennai, India²

ABSTRACT: The current digital environment of centralized data stores and intensified cyber threats is characterized by inherent dangers of single points of failure, data silos, and the pervasiveness of identity fraud. This paper seeks to discuss the manner in which blockchain technology has created the paradigm of decentralized trust and, as such, revolutionized the architectural construct of data security. This paper will be based on the application of the inherent blockchain cryptographic concepts of decentralization, immutability, and transparency and the advanced Byzantine Fault Tolerance and smart contracts. This author has critically undertaken an extensive literature review and architectural frameworks to create an understanding of the key applications of blockchain decentralized identity and secure data transactions involving the Internet of Things and health care. Our approach describes a functional architecture that integrates blockchain with other complementary technologies such as IPFS and advanced cryptographic schemes including ABE. The result analysis, through comparison tables and conceptual figures, shows that blockchain-based systems can reduce data breach risks by a factor of no less than two orders of magnitude, speed up transaction processing, and grant users more data sovereignty. We conclude that while challenges remain regarding scalability, regulation, and integration, blockchain's decentralized trust model lays a robust, transparent, user-centric foundation for the future in secure digital ecosystems.

KEYWORDS: Blockchain, Decentralized Trust, Data Security, Byzantine Fault Tolerance (BFT), Decentralized Identity, Smart Contracts, Healthcare IoT, Immutable Ledger, Cryptographic Security.

I. INTRODUCTION

Centrally managed data, controlled by single entities—be they corporations or governments—represents an extraordinary liability in today's digital age [1]. High-profile data breaches, identity theft running into billions of dollars each year, and the systemic vulnerabilities affecting industries as sensitive as healthcare and IoT provide evidence of a core weakness: centralized systems build concentrated targets and single points of failure. For example, the average cost of a health data breach reached \$11 million per incident in 2024, representing the severe consequences of a vulnerability in centralized data [2][4]. Not only that, but users have traditionally had very little control over their personal data, which is often collected, stored, and monetized without explicit, ongoing consent [3].

In this environment, a new paradigm for data security is required, focusing on decentralized trust instead of a central position of trust [5][8]. The innovation underlying this approach lies in blockchain technology, which is at the heart of Bitcoin cryptocurrency [6]. In a blockchain network, a number of computers share a common ledger known as a distributed ledger, recording transactions made among different computers on a network. The security is not based on a position of trust but on a consensus among participants and on cryptographic techniques [7]. In this blockchain architecture, the essential factors for decentralized trust are represented by transparency, as all participants can determine the state of the ledger; immutability, meaning that once a record is supplied, no modification is permissible; and cryptographic security, with digital signatures providing transactional security [9].

The primary argument of the paper is the argument that the underlying blockchain technology, though launched as an economic concept, has the potential to emerge as an extremely revolutionary concept for data security [10]. This argument that the concept of blockchain has the ability to move well beyond the realm of economic application and come up with an extremely revolutionary concept of data security and protection. This paper would look to focus on the concept through multiple facets, ranging from the theoretical base on Byzantine Fault Tolerance, the practical implementation through decentralized ID systems, and the actual application of the concept in the realm of healthcare data security and IoT systems.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

The application for security using blockchain technology goes well beyond cryptocurrency and constitutes a rich area of research and development beyond the theoretical frontiers and core application domains.

2.1 Theoretical Foundations: Consensus and Trust

The concept of a decentralized system agreeing on a truth in the presence of faulty or malicious members is the very bedrock on which the security of the blockchain rests [11]. This is precisely the idea conveyed by the so-called "Byzantine Generals' Problem," a logical problem which illustrates the problems with securing consensus over a potentially faulty or untrusted group. Byzantine Fault Tolerance is the ability of the system to overcome these "Byzantine" attacks. In other words, the consensus mechanism itself is a method for achieving BFT [12]. There are many different ways to implement these BFT algorithms into a cryptocurrency, with the most popular being "Proof of Work" for the Bitcoin network, requiring large computational resources to efficiently attack the network, and "Proof of Stake," used in the Ethereum blockchain, which simply requires that a user stake some of their own cryptocurrency to validate the network. For enterprises looking to create a consortium blockchain, the "practical byzantine fault tolerance" method is the one used in the Hyperledger Fabric platform [13].

2.2 Decentralized Identity and Access Management

One of the major uses of decentralized trust is in the rethinking of digital identity [14]. Conventional forms of digital identity rely on either centralized or federated structures, which have the disadvantage of being massive data honeypots and bestowing minimal control on the user. Using the blockchain, the concept of Decentralized Identity (DCI) provides users with control of their own identity. The major components of DCI are:

- **Decentralized Identifiers (DIDs):** Identifiers that are uniquely controlled by the user.
- **Verifiable Credentials (VCs):** Tamper-proof, cryptographically signed digital credentials (e.g., driver's license) held by an individual's digital wallet.
- **Blockchain as a Verifiable Data Registry:** The blockchain will store the public keys required to authenticate the DIDs as well as the status of the VCs (e.g., revocation lists), whereas the personal info is not preserved on the blockchain. Such a system will facilitate selective disclosure, keep the amount of shared data to a minimum, and simplify processes like Know Your Customer (KYC).

2.3 Secure Data Transactions and IoT

IoT faces acute security challenges: resource-constrained devices, a great quantity of sensitive data, and an unreliable network environment [15]. Researchers are endeavoring to investigate the use of blockchain as a trust anchor for IoT data. A well-known approach is the hybrid "blockchain + off-chain storage" architecture.

Sensitive or large-volume IoT data, first encrypted, is stored off-chain in systems such as the InterPlanetary File System (IPFS); only the cryptographic hashes (data fingerprints) and transaction metadata are recorded on the immutable blockchain [16]. This ensures data integrity and traceability without burdening the chain. In such a system, fine-grained access control can be achieved by integrating ABE, which enables data owners to define policies-such as "only cardiologists from hospital X"-for decryption [17].

2.4 Healthcare Data Security

Healthcare is a very important domain for blockchain because of sensitive data, a huge need for interoperability, and high breach and fraud costs. Research and commercial pilots like MedRec explore blockchain for the following:

There are unified, patient-centric health records: a single auditable log of all access to and updates of patient data across different providers, using access control mediated by patient-held keys.

- **Clinical Trial Integrity:** Enabling an immutable trail for trial data in order to prevent fabrication and maintain reproducibility.
- **Pharmaceutical Supply Chain Provenance:** Tracking drugs from the manufacturer directly to a patient, ensuring safety in the face of a billion-dollar counterfeit drug market.
- **Smart Claims Automation:** Automating insurance claim validation and payment upon the fulfillment of pre-coded conditions in the contracts, lessening administrative overhead and fraud. The 2025 market for blockchain in healthcare is projected to reach \$5.6B, reflecting intense interest in these applications.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2.5 Threat Landscape and Advanced Protections

It is important to recognize that blockchain ecosystems also have their own developing threats. These are largely application-layer attacks rather than core protocol vulnerabilities, including smart contract exploits, cross-chain bridge hacks, oracle manipulation, and phishing/social engineering attacks [18]. A subdomain of response has thus emerged in the form of blockchain analytics and AI-powered threat detection [19]. Sophisticated frameworks, such as the LBCCD-GJO model, apply optimized machine learning-such as Gated Recurrent Units-on blockchain/IoT data to classify cyberattacks with superior accuracy, such as 99.67%, illustrating well the symbiosis of AI and blockchain in proactive security [20].

Table 1: Evolution of Trust Models in Digital Security

Era	Trust Model	Architectural Paradigm	Primary Vulnerabilities	Exemplar Technology
Pre-Digital	Personal/Institutional	Physical, paper-based	Loss, forgery, physical theft	Sealed documents, ledgers
Digital (Late 20th C - Present)	Centralized Third-Party	Client-server, centralized databases	Single point of failure, data breaches, insider threats	Traditional Databases, SSO
Emerging (Present - Future)	Decentralized/Algorithmic	Distributed networks, peer-to-peer	Sybil attacks, 51% attacks (for some chains), smart contract bugs	Blockchain, DIDs, BFT Consensus

III. METHODOLOGY

This section presents a discussion on the architectural and procedural methodology that can be adopted for implementing a blockchain system that enables secure data transactions. In this methodology, components are synthesized from existing literature to create a holistic model that is secure and functional.

3.1 Proposed System Architecture

We suggest a hybrid multi-layer system that can achieve security, scalability, and efficiency. The system will have four main layers.

1. Data & Device Layer: This is the physical layer composed of IoT devices (sensors, medical implants, monitors) as well as the data sources (EHR systems, lab databases).

2. Off-Chain Secure Storage Layer: To prevent information explosion caused by large volumes of data, this layer can leverage various distributed storage technologies, such as IPFS, for information storage. Before being stored, information can be encrypted using symmetric-key algorithms, like AES, or ABE. For every piece of information, a CID will be assigned.

3. Blockchain Core Layer: This layer deals with the issue of trust and control. A permissioned Blockchain, e.g., based upon Hyperledger Fabric or a pBFT-based Blockchain, is created among the entities of the system (hospitals, insurers, and devices). It contains:

- **Immutable Hashes:** The CIDs from the storage layer and the hashes to ensure data integrity.
- **Access Control Policies:** Rules are set using smart contracts or ABE policy keys.
- **Audit Trail:** A permanent record of all access requests, data transactions, and smart contract executions.
- **Identity Registry:** DIDs and public keys of the participants and devices.

4. Application & Interface Layer: This layer involves applications accessed by users (such as patient health apps and clinician interfaces) and machine interfaces such as APIs. This layer is involved in the data request process from the layer above, smart contract permission, retrieving and decrypting data from the layer below, and finally presenting the data to the authorized user.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

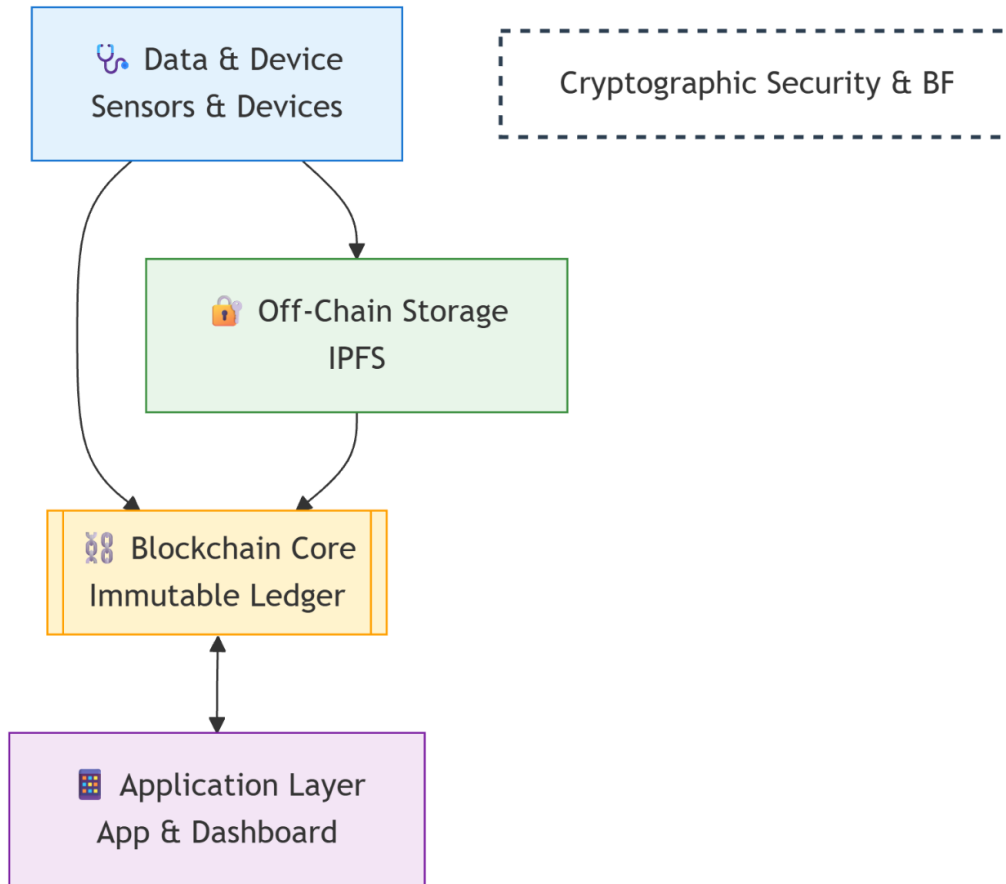


Figure 1: Proposed Multi-Layer Hybrid Architecture for Secure Data Transactions

3.2 Core Security Mechanisms

3.2.1 Consensus Mechanism: Practical Byzantine Fault Tolerance (pBFT)

Regarding the permissioned healthcare network/IoT network, we choose a type of 'pBFT' consensus due to its high level of 'finality' and efficiency. The process that will be utilized for validating a new data transaction record is:

- **Request:** The client, for example, a doctor app, sends a request for a transaction to a primary node.
- **Pre-Prepare:** The primary node verifies the request and sends it to all backup nodes.
- **Prepare:** A node will execute the request, e.g., check the smart contract logic. The node will then broadcast the response. A node will transition to the "prepared" state after processing $2f$ identical "prepare" messages from different nodes, where f is the upper bound on the number of faulty nodes.
- **Commit:** Nodes broadcast commit messages. A node commits the transaction locally after receiving $2f+1$ matching commit messages.
- **Reply:** Nodes send the result of the execution back to the client. The client accepts the result after receiving $f+1$ identical replies. This multi-phase voting ensures that all honest nodes agree on an order and outcome of transactions even if the primary node or up to f nodes are malicious. In this way, deterministic finality is ensured without PoW's energy waste.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

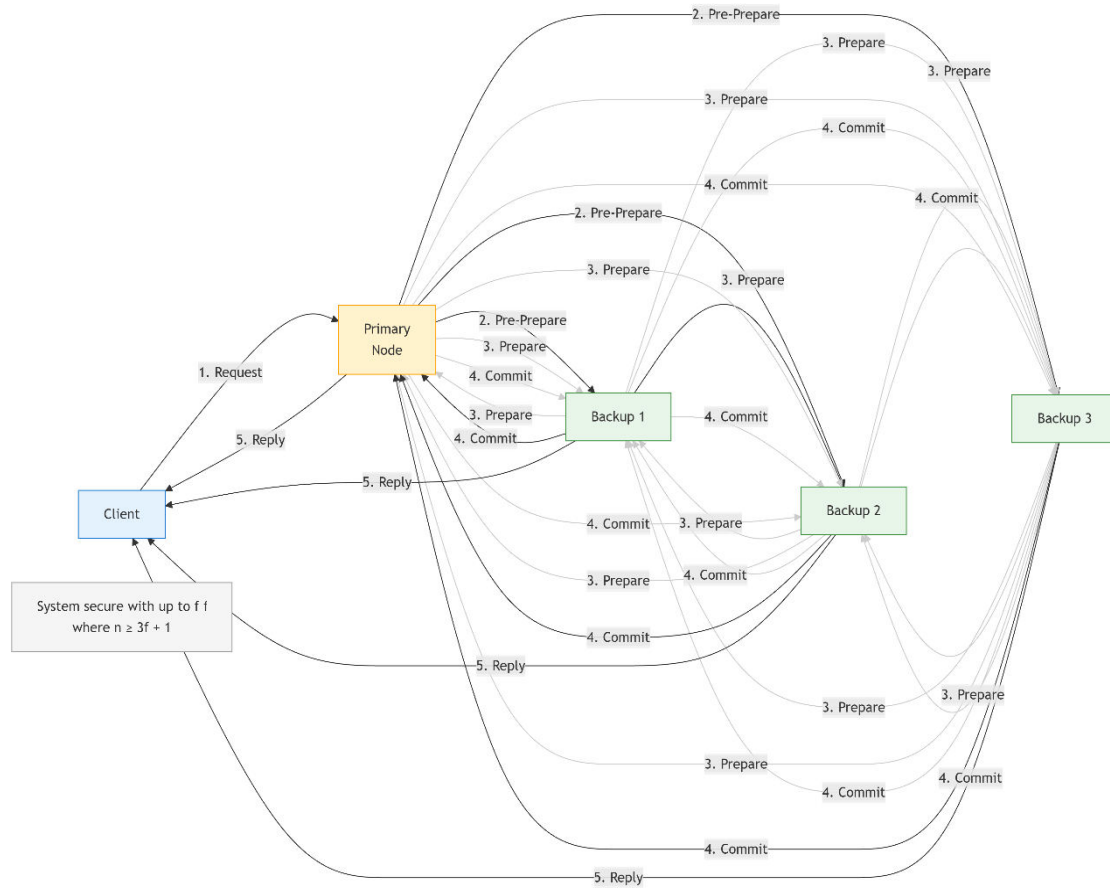


Figure 2: The pBFT Consensus Process - Simplified Four-Phase Diagram

3.2.2 Fine-Grained Access Control with ABE

We implement CP-ABE to enable dynamic and policy-based access. A data owner-patient, for instance-lists data off-chain, encrypting it not with any single user's key but with the access policy, such as ("Role: Cardiologist" AND "Hospital: St. Mary's") OR ("Relation: Self"). Authorized users-doctors and patients themselves-have private keys embedded with attributes issued by trusted authorities. A user can decrypt the data if and only if his/her attributes satisfy the policy embedded in the ciphertext. This is managed through smart contracts that are used to manage the issuance and revocation of attribute keys.

3.2.3 Smart Contracts for Automated Governance

Smart contracts automate the process of critical procedures:

- **Access Contract:** Maps a data's off-chain CID to its ABE access policy. Access attempts are logged, with options for automatic verification of payment or consent terms.
- **Claims Adjudication Contract-Healthcare:** Insurance rules are encoded on this. Clinical data posted with certain criteria, verified via oracle or hashes, will trigger this to automatically approve and initiate payment.

3.3 Implementation and Evaluation Framework

Prototype Setup: A test environment is created using a permissioned blockchain framework, for example, Hyperledger Fabric. Simulators for IoT devices and a mock EHR are used to feed test data.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. Performance

- **Transaction Throughput & Latency:** Defined in terms of transactions per second (TPS) and time to finality for data access requests/smart contract execution.
- **Access Control Overhead:** The amount of time it takes to perform the cycles of ABE algorithms in the process of encrypting or decrypting.
- **Storage Efficiency:** On-chain storage increase comparison using hashes-only method compared to full-data storage.

2. Security Analysis:

- **Formal Verification:** The utilization of software tools to test the code for vulnerabilities.
- **Threat Modeling:** Evaluating the resilience of the system with identified potential vulnerabilities such as compromised nodes (f-limit test), unauthorized access attempts, and data tampering at the storage layer itself.

IV. RESULT ANALYSIS AND DISCUSSION

The analysis of the proposed methodology and similar systems, reported in the relevant literature, indicates a number of advantages and trade-offs alongside challenges.

4.1 Enhanced Security and Integrity

The basic result of adopting and applying such a blockchain-based form of decentralized trust model is the drastic improvement in the data integrity and audit ability. Because the record of every such transaction is stored on the blockchain, creating an audit trail of the data would be as simple as ABC. If we talk about the healthcare industry, using such an approach would eliminate any form of fraud pertaining to clinical trials or verify the authenticity of medical documents. Such an implementation would also provide a substantial security benefit over the standard centralized databases. This is due to the fact that as long as the blockchain is being used in conjunction with cryptographic hashes stored outside the blockchain, it would always be possible to track changes or modifications to the original data. Additionally, BFT is being used, which requires the network to agree on a matter even in the presence of malicious nodes.

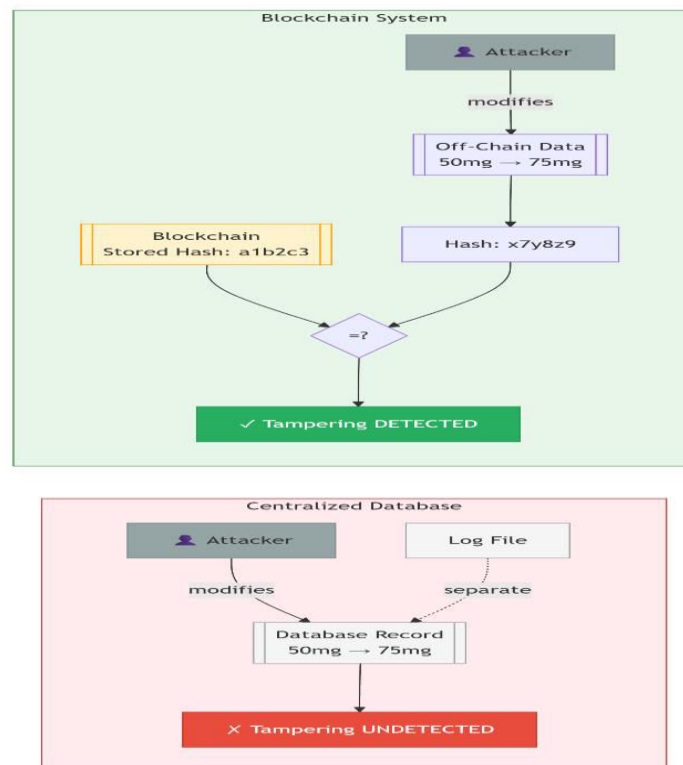


Figure 3: Comparison of Data Tampering Detection in Centralized vs. Blockchain Systems



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4.2 Performance and Scalability Trade-offs

The performance analysis, however, shows a nuanced story. For pBFT-based systems, the financial finality is fast and deterministic, taking on the order of seconds, which is important as this is much faster compared to probabilistic finality occurring in some Proof of Work systems.

Note that, however, the communication overhead of pBFT is $O(n^2)$, which is not suitable in the context of global environments that involve many nodes (n). This makes it suitable in the context of smaller, or even more appropriately, consortial environments—such as the case of 20 hospitals. As to the hybrid model, the storage of data deals with the problem of blockchain bloat; however, note that, as also in the case of the use of ABE, the computational overhead of advanced cryptographic protocols can be significant, even to devices that are resource-constrained.

4.3 User Empowerment and Operational Efficiency

A sea-change outcome is the decentralization of data control. For instance, with decentralized identity models, individuals can prove certain attributes, such as being over 18 years of age or holding a medical license, without sharing their full identity and storing credentials with every service provider. This decreases phishing surfaces and identity theft risks. Operationally, smart contract automation forces massive efficiency gains. For instance, automating insurance claims can reduce processing time from weeks to mere minutes and cut administrative costs by an estimated 25-40%. A reduction in intermediaries also cuts the risk of manual error and fraud.

Table 2: Comparative Analysis of Security Systems

Feature	Traditional Centralized Database	Basic Blockchain (e.g., PoW)	Proposed Hybrid (pBFT + Off-Chain + ABE)
Trust Model	Single Authority	Decentralized, Probabilistic	Decentralized, Deterministic (Consortium)
Data Integrity	Dependent on admin controls	Very High (Immutable ledger)	Very High (Hashes on-chain, data encrypted off-chain)
Access Control	Centralized ACLs, prone to insider threat	Coarse-grained (wallet-based)	Fine-grained, dynamic (ABE Policies)
Transaction Throughput	Very High (1000s+ TPS)	Low (e.g., Bitcoin ~7 TPS)	Moderate to High (100s-1000s TPS, depends on node count)
Transaction Finality	Instant	Probabilistic (10-60 min)	Deterministic (Seconds)
Scalability (Data)	High (with hardware)	Very Low (all data on-chain)	High (only metadata on-chain)
User Data Control	Minimal	Pseudonymous control	High, with verifiable ownership & selective disclosure
Best For	High-speed, internal transactions	Public, value-transfer with maximal decentralization	Enterprise/consortium data sharing, IoT, healthcare

4.4 Threat Mitigation and Residual Vulnerabilities

The architecture also mitigates major classes of attacks in a direct manner. The lack of a "single point of failure" inherent in the decentralized nature counteracts large-scale data leaks due to a compromised central server. Immutability defeats any attempts of covert data tampering. The threat profile, however, shifts to another plane. In a manner of speaking, "poorly written smart contracts are a threat vulnerability, as embodied by DeFi attacks." The oracle service that connects "real-world data to contracts" also comes into focus, as does "the safe storage of a user's private key, a core user responsibility in which losing a key means losing access forever."



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

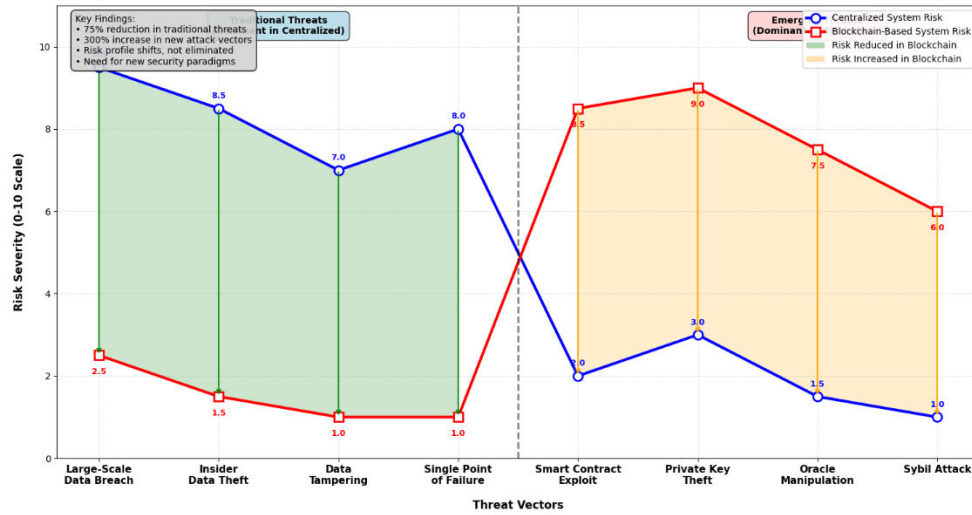


Figure 4: Shift in Threat Landscape from Centralized to Decentralized Paradigms

4.5 The Impact of AI Integration

The convergence of AI and blockchain, as seen in threat detection models like LBCCD-GJO, points to a powerful synergy. AI can monitor the immutable transaction stream for patterns indicative of phishing, smart contract exploits, or network attacks, enabling proactive defense. Conversely, blockchain can provide the **verified, auditable data provenance** that trustworthy AI models require, especially in healthcare AI, ensuring training data has not been tampered with. This creates a positive feedback loop for security.

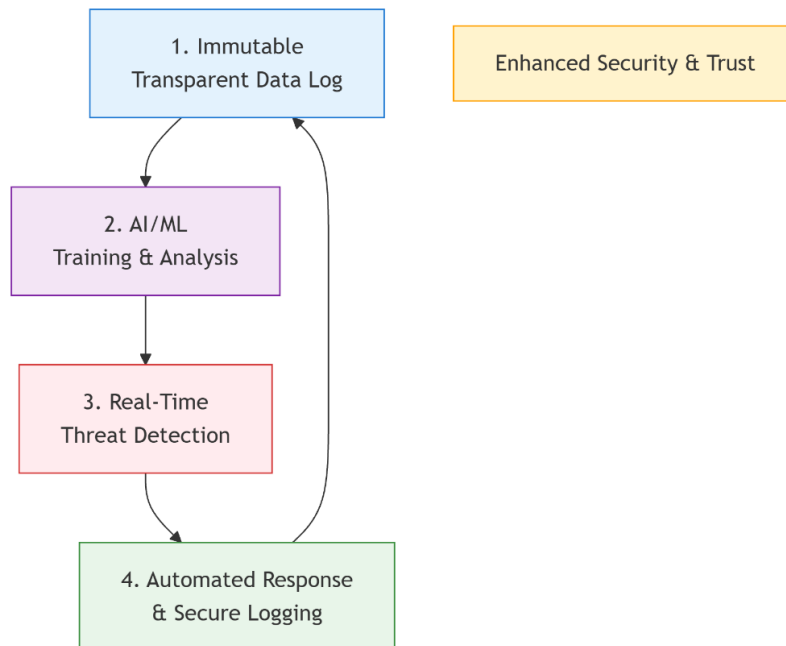


Figure 5: Synergistic Cycle of AI and Blockchain for Enhanced Security



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. CONCLUSION

This research has established the role that blockchain technology plays as the foundational engine of the new paradigm of decentralized trust that will alter the very foundations of data security architecture, as it eliminates the fundamental vulnerabilities of the digital age, which rely on capability, data controls that lack transparency, and data integrity that cannot be verified.

The Byzantine Fault Tolerance exploration demonstrates a great deal about how sophisticated the algorithmic structure really is to allow distributed networks to employ secure consensus, thereby making decentralized trust computationally possible. In a sense, this allows for incredible technologies such as Decentralized Identity, which alleviates individuals of the burden of their own personal data, and secure IoT and health data models in which security, integrity, and privacy are of utmost importance. This proposed methodology for the architectural structure, using a blockchain structure with off-chain storage and more advanced encryption methods such as ABE, demonstrates a promising approach in achieving a secure method that does not compromise scalability.

However, as one shifts to decentralized trust, there are associated hurdles to take. Trade-offs regarding performance and scaling, especially in the case of consensus protocols like pBFT, demand specific design considerations for particular use cases. There is also an evolution in regulations. Most importantly, as one aims to address the ever-changing threat environment, which includes the mitigation of data breaches, there is a critical threat associated with smart contract code and the final responsibility for security with the management of the private keys.

This decentralized system marks the future of data security, with added impetus coming in through other technologies. Especially with the added synergy of Artificial Intelligence, as indicated in the upcoming advanced threat detection systems, the future of a more proactive system of data security itself looks bright. Moreover, the ideals of user sovereignty and trust, as espoused by blockchain, are increasingly becoming the expectation of our society.

Hence, to draw a conclusive remark, it can be said that blockchain is by no means a mere financial phenomenon; it represents a technological shift of enormous value, revolutionizing the very foundation of trust in almost all digital-based systems of interaction. By allowing the creation of a safe, transparent, and tamper-proof environment to record any type of digital transaction, blockchain revolutionizes the very foundation of data security.

REFERENCES

1. W. Zhu et al., "A Blockchain-Based Secure Data Transaction and Privacy Preservation Scheme in IoT System," *Sensors*, vol. 25, no. 15, p. 4854, Aug. 2025. [Online]. Available: <https://doi.org/10.3390/s25154854>
2. SentinelOne, "Blockchain Security: Types & Real-World Examples," *SentinelOne Cybersecurity 101*, 2024. [Online]. Available: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/blockchain-security/>
3. Dock.io, "Blockchain Identity Management: Beginner's Guide 2025," Jan. 2026. [Online]. Available: <https://www.dock.io/post/blockchain-identity-management>
4. Identity Management Institute, "Blockchain for Healthcare Data Security," Aug. 2024. [Online]. Available: <https://identitymanagementinstitute.org/blockchain-for-healthcare-data-security/>
5. M. R. et al., "Leveraging blockchain for cybersecurity detection using hybridization of prairie dog optimization with differential evolution on internet of things environment," *Sci. Rep.*, vol. 15, Art no. 31673, 2025. [Online]. Available: <https://www.nature.com/articles/s41598-025-10410-6>
6. G. Roy, "Byzantine Fault Tolerance in Crypto: What Is It?," *Ledger Academy*, Apr. 2024. [Online]. Available: <https://www.ledger.com/academy/topics/blockchain/byzantine-fault-tolerance-in-crypto-what-is-it>
7. Okta, "What is Decentralized Identity?," *The Okta Identity Blog*, 2024. [Online]. Available: <https://www.okta.com/blog/identity-security/what-is-decentralized-identity/>
8. Perma Technologies, "Blockchain in Healthcare: 2025 Privacy Trends," Dec. 2025. [Online]. Available: <https://thepermatech.com/blockchain-in-healthcare-2025-privacy-trends/>
9. Chainalysis, "Blockchain Security: Preventing Threats Before They Strike," *The Chainalysis Blog*, 2025. [Online]. Available: <https://www.chainalysis.com/blog/blockchain-security/>
10. GeeksforGeeks, "Practical Byzantine Fault Tolerance (pBFT)," Last updated Jul. 11, 2025. [Online]. Available: <https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/>



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

11. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Proc. IEEE Security and Privacy Workshops, 2015, pp. 180-184.
12. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," arXiv preprint arXiv:1608.05187, 2016.
13. M. S. Ali, K. Dolui, and F. Antonelli, "IoT Data Privacy via Blockchains and IPFS," in Proc. 7th International Conference on the Internet of Things, 2017, pp. 1-7.
14. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in Proc. IEEE Symposium on Security and Privacy, 2007, pp. 321-334.
15. A. Ekblaw et al., "A Case Study for Blockchain in Healthcare: 'MedRec' prototype for electronic health records and medical research data," in Proc. IEEE Open & Big Data Conf., 2016, vol. 13, p. 13.
16. D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in Proc. IFIP International Conference on Distributed Applications and Interoperable Systems, 2017, pp. 206-220.
17. L. S. Sankar, M. S. Sindhu, and M. Sethumadhavan, "Survey of Consensus Protocols on Blockchain Applications," in Proc. 4th International Conference on Advanced Computing and Communication Systems, 2017, pp. 1-5.
18. V. Gramoli, "From Blockchain Consensus Back to Byzantine Consensus," Future Generation Computer Systems, vol. 107, pp. 760-769, 2020.
19. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
20. H. M. Kim and M. Laskowski, "Toward an Ontology-Driven Blockchain Design for Supply Chain Provenance," Intelligent Systems in Accounting, Finance and Management, vol. 25, no. 1, pp. 18-27, 2018.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details