# PERFORMANCE ANALYSIS OF BIGDATA SECURITY IN BLOCKCHAIN TECHNOLOGY

**K. Kaviya [1], T. Sangeetha [2], Avinash. P [3]**

[1] Assistant Professor, Department of Computer Science Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu, Tamil Nadu, India

[2] Associate Professor, Department of Biomedical Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu, Tamil Nadu, India

[3] Student, Department of Artificial Intelligence and Data Science, Karpaga Vinayaga College of Engineering and Technology, Chengalpattu, Tamil Nadu, India

## ABSTRACT

In today's digital age, it is common for parties to exchange sensitive information. Banking information, insurance data, and health records are just a few instances of sensitive data or documents that necessitate a digital interchange. In many circumstances, the transaction takes place between unidentified and untrustworthy persons. As a result, executing the data exchange using a fair non-repudiation protocol is critical. Non-repudiation is indisputable proof of one's accountability for the veracity of whatever data he shares/receives in digital communication. This is usually accomplished via the use of a cryptographic digital signature. Neither side can deny that their digital signature is legitimate in this situation. At every point throughout the exchange process, the protocol meets the fairness property if and only if it does not provide the sender any benefits over the receiver or vice versa. In many applications, combining fair exchange and non-repudiation for digital trade is crucial, and it may be obtained with or without the use of a trusted third party (TTP). Fairness becomes probabilistic without TTP's participation, and TTP's inclusion might lead to excessive dependency on the third party. In many applications, a peer-to-peer (P2P) fair nonrepudiation protocol that does not rely on a trusted third-party is desired. The blockchain network is built in such a manner that it can manage a trust less environment while still delivering the proper result. As a result, if the exchanges are conducted using Blockchain, genuine fairness will be ensured, and none of the parties would have to deal with the problem of trust. An ever-increasing amount of sensitive patient information is shared between healthcare institutions.The proposed methodology is experimentally tested and validated with the existing techniques regarding encryption time, decryption time, throughput, delay, and overall processing time.

## KEYWORDS

Blockchain technology - Electronic health records– sensitive information- Trusted third party

# I. INTRODUCTION

Healthcare recordkeeping systems serve as the foundation for modern medical care, allowing for the seamless storage and retrieval of patient information across various healthcare settings. These systems must adhere to the highest standards of auditability and privacy to protect sensitive patient data. Traditional electronic health records (EHRs) contain extremely sensitive information that needs to be shared securely among healthcare professionals. The integration of blockchain technology addresses many of the security concerns associated with EHRs by providing a decentralized, immutable system where data cannot be tampered with. Each block in the chain contains a computed hash of the previous block's contents, creating a dependency that ensures data integrity. The distributed consensus mechanisms allow nodes to maintain synchronized copies of the blockchain, further enhancing security and reliability.

## A. UNDERSTANDING ARTIFICIAL INTELLIGENCE IN HEALTHCARE

Artificial intellect involves the development of computer systems capable of doing activities that traditionally require human intellect. In healthcare, AI manifests through various functions including learning from patient data patterns, solving complex diagnostic problems, making treatment recommendations, and perceiving subtle indicators in medical imaging. AI systems can analyze vast datasets of medical information to identify trends and correlations that might escape human observation. These capabilities make AI particularly valuable for enhancing clinical decision support, personalizing treatment plans, automating administrative tasks, and improving diagnostic accuracy. The adaptive nature of AI algorithms means they can continuously improve their performance as they process more healthcare data, leading to increasingly sophisticated applications in medical practice.

## B. BENEFITS OF AI-BLOCKCHAIN INTEGRATION IN HEALTHCARE RECORDS

The integration of AI with blockchain technologies creates powerful synergies that address critical challenges in healthcare recordkeeping. AI-powered algorithms significantly enhance security by detecting anomalous access patterns and preventing unauthorized attempts to access sensitive medical information. The scalability of healthcare data systems improves substantially when AI optimizes blockchain networks, enabling faster processing of medical transactions and accommodating the ever-increasing volume of healthcare data. Smart contracts within healthcare blockchain systems benefit from AI analysis that reduces errors in automated processes such as insurance claims or medication management protocols. Predictive maintenance capabilities powered by AI ensure continuous availability of healthcare records, preventing system downtime that could compromise patient care in critical situations. Additionally, AI-driven analytics applied to blockchain-secured health records can identify population health trends while maintaining individual privacy protections.

## C. APPLICATIONS IN ELECTRONIC HEALTH RECORD MANAGEMENT

AI-powered blockchain solutions transform EHR management by creating comprehensive, secure patient records that follow individuals throughout their healthcare journey. These integrated systems enable seamless interoperability between different healthcare providers while maintaining strict access controls through smart contract mechanisms. Patients gain unprecedented control over their medical information, using cryptographic keys to grant temporary access to specific providers. The immutable nature of blockchain creates an auditable trail of all record access and modifications, ensuring regulatory compliance and building trust among stakeholders. AI algorithms working within this blockchain framework can automatically categorize and prioritize

information within health records, presenting healthcare providers with the most relevant data for each clinical encounter. This intelligent information management reduces cognitive burden on clinicians while improving the quality of care decisions.

## D. IMPLEMENTATION IN PERSONALIZED MEDICINE AND RESEARCH

The combination of AI and blockchain technologies creates powerful opportunities for advancing personalized medicine. Securely anonymized patient data stored on blockchain systems can be analyzed by AI algorithms to identify subtle patterns that inform precision treatment approaches. Researchers can access broader datasets than previously possible, with blockchain providing transparent consent management and compensation mechanisms for data contribution. AI models trained on these diverse datasets develop more sophisticated understanding of disease manifestations across different demographic groups. Blockchain's immutable record of data provenance ensures research integrity, while AI streamlines the integration of findings back into clinical practice through continuously updated treatment protocols. This creates a virtuous cycle where clinical care informs research, and research rapidly improves clinical outcomes through AI-mediated knowledge transfer.

## E. ADDRESSING PRIVACY AND REGULATORY COMPLIANCE

The integration of AI and blockchain in healthcare recordkeeping introduces sophisticated approaches to privacy protection and regulatory compliance. Blockchain's cryptographic protection of patient identities, combined with AI's ability to detect potential privacy breaches, creates a robust security framework. Healthcare organizations can demonstrate HIPAA compliance through the transparent audit trails inherent in blockchain systems, while AI-powered monitoring ensures continuous adherence to regulatory requirements. Smart contracts automatically enforce data usage policies, preventing improper information sharing even when multiple organizations contribute to patient care. Furthermore, AI algorithms can selectively anonymize sensitive information for research purposes while preserving the clinical utility of the data. As regulatory frameworks evolve to address emerging technologies, the flexibility of AI-blockchain systems allows for rapid adaptation to new compliance requirements without disrupting clinical operations.

## F. CHALLENGES IN TECHNICAL IMPLEMENTATION

Despite the promising potential, implementing AI-blockchain solutions in healthcare faces significant technical challenges. The computational intensity of both technologies creates scalability concerns, potentially limiting performance during periods of high demand for healthcare services. Healthcare data quality varies considerably across providers and systems, potentially compromising the effectiveness of AI algorithms trained on blockchain-stored records. Legacy systems prevalent in healthcare organizations may resist integration with cutting-edge blockchain platforms, necessitating complex middleware solutions. The energy consumption associated with certain blockchain consensus mechanisms raises sustainability concerns for healthcare institutions with limited resources. Additionally, the distributed nature of blockchain networks introduces latency that may be problematic in emergency care situations where immediate access to complete records is critical. Addressing these challenges requires thoughtful architectural decisions and possibly the development of healthcare-specific consensus mechanisms that balance security with performance requirements.

### G. SOCIOECONOMIC AND ADOPTION CONSIDERATIONS

The widespread implementation of AI-blockchain healthcare record systems depends on numerous socioeconomic factors beyond technical feasibility. Healthcare professionals require specialized training to effectively utilize these advanced systems, creating potential workforce development challenges. The initial investment for implementing comprehensive AI-blockchain infrastructure may be prohibitive for smaller healthcare providers, potentially exacerbating existing disparities in healthcare quality. Patient acceptance depends on clear communication about how their data is secured and utilized, requiring transparent explanations of complex technological processes. Differing international regulatory approaches to healthcare data management complicate implementation for organizations operating across borders. Furthermore, equitable access to the benefits of these advanced systems requires careful consideration of digital divide issues, ensuring that technological advances don't inadvertently create new healthcare inequalities. Successful adoption strategies must address these socioeconomic factors alongside technical implementation challenges.

### H. FUTURE DIRECTIONS AND EMERGING APPLICATIONS

The future of AI-blockchain integration in healthcare recordkeeping promises increasingly sophisticated applications that transform medical practice. Emerging developments include AI-powered predictive analytics operating on blockchain-secured longitudinal health records to anticipate individual health deterioration before symptoms appear. Decentralized AI models may evolve collaboratively across blockchain networks while preserving data privacy, creating increasingly powerful diagnostic tools without centralizing sensitive information. Internet of Medical Things (IoMT) devices could securely contribute real-time patient monitoring data to blockchain records, with AI providing immediate analysis and alerts. Blockchain-based systems might facilitate novel healthcare delivery and payment models, using AI to match patients with appropriate services while automatically managing compensation through cryptocurrency transactions. As quantum computing advances, new cryptographic methods will emerge to maintain blockchain security against increasingly powerful computational attacks. These emerging applications suggest that the intersection of AI and blockchain will continue to drive innovation in healthcare information management for decades to come.

## II. BIG DATA

### A. UNDERSTANDING BIG DATA: DEFINITIONS AND SCOPE

Big Data has emerged as a pivotal concept in the information technology landscape, encompassing vast collections of heterogeneous information that expand at unprecedented rates and volumes. The term refers to significant amounts of structured, quasi-structured, unstructured, and semi-structured data that can be leveraged for machine learning projects and advanced analytics applications. What distinguishes Big Data from conventional data management is not merely its volume but also its variety and velocity—often referred to as the three Vs. The variety aspect acknowledges the diverse formats data can take, from traditional structured database entries to unstructured text, images, videos, and sensor readings. Velocity refers to the speed at which data is generated, collected, and processed, which has accelerated dramatically with the proliferation of digital devices and internet connectivity. As organizations increasingly recognize the competitive advantage that can be gained through effective data

utilization, they are investing heavily in infrastructure and expertise to harness these massive information repositories for commercial purposes and strategic decision-making.

## B. CHALLENGES IN BIG DATA STORAGE ARCHITECTURE

Storage infrastructure for Big Data presents unique technical challenges that extend beyond simply scaling up traditional database systems. The rapid generation of data creates a constant pressure on storage systems, requiring them to maintain high throughput and processing capabilities while handling diverse data formats simultaneously. Organizations must implement storage architectures specifically designed to accommodate the three Vs of Big Data without compromising on performance or reliability. These specialized storage systems must integrate seamlessly with data processing frameworks and analytics platforms to ensure efficient data accessibility. The heterogeneous nature of Big Data further complicates storage decisions, as different data types may require different optimization strategies—some prioritizing retrieval speed while others emphasizing space efficiency or data integrity. Storage solutions must also be designed with future scalability in mind, allowing for horizontal expansion as data volumes continue to grow exponentially. This architectural complexity represents a significant investment challenge for many organizations, particularly those transitioning from legacy systems to Big Data-ready infrastructure.

## C. DISTRIBUTED STORAGE SYSTEMS FOR BIG DATA

Modern Big Data storage implementations typically rely on distributed architectures that spread data across multiple nodes or servers, creating resilient systems capable of handling massive volumes. Distributed file systems like Hadoop Distributed File System (HDFS) have become foundational components of many Big Data ecosystems, allowing organizations to store petabytes of information across commodity hardware clusters. These systems employ data replication strategies to ensure fault tolerance, maintaining multiple copies of each data block across different physical machines. Data partitioning techniques further enhance performance by distributing computational workloads across the cluster, enabling parallel processing that significantly reduces analysis time for large datasets. Cloud-based distributed storage solutions have also gained popularity, offering scalable capacity with reduced upfront infrastructure investment. These systems provide flexibility through virtualized storage resources that can be provisioned on demand as data requirements evolve. The distributed nature of these storage architectures aligns perfectly with distributed processing frameworks, creating cohesive ecosystems where data locality optimizations further enhance analytical performance by minimizing data movement during computation.

## D. STORAGE MANAGEMENT AND DATA ACCESSIBILITY

Effective Big Data storage extends beyond mere capacity to encompass sophisticated management capabilities that ensure data remains accessible and usable. Metadata management plays a crucial role in this context, providing the indexing and cataloging necessary to locate specific information within vast data lakes. Data lifecycle management systems automatically

migrate information between storage tiers based on access patterns and aging policies, optimizing storage costs while maintaining appropriate access performance for different data categories. Data virtualization technologies create abstraction layers that shield applications from the underlying storage complexity, presenting unified views of information scattered across heterogeneous storage systems. Advanced caching mechanisms further enhance performance by maintaining frequently accessed data in high-speed memory, reducing latency for common queries. The challenge of data accessibility also extends to integration capabilities, as Big Data systems must often interface with traditional enterprise data sources while maintaining consistency and synchronization. Organizations implementing Big Data storage must therefore develop comprehensive data governance frameworks that address not only the technical aspects of storage but also data quality, security, and compliance considerations to ensure that stored information remains valuable and trustworthy throughout its lifecycle.

# III. DATA LAKES

A data lake represents a revolutionary approach to enterprise data storage, functioning as a centralized repository that houses vast amounts of raw information in its native format until processing is required. Unlike traditional data warehouses that impose rigid structures before storage, data lakes embrace the diversity of data formats, accommodating structured data from relational databases, semi-structured information like CSV files, logs, XML and JSON documents, unstructured content such as emails, documents, and PDFs, as well as binary data including images, audio, and video files. This inclusive approach creates a comprehensive organizational memory that preserves data in its original form, maintaining all inherent information without the potential loss that can occur during premature transformation. The fundamental philosophy behind data lakes acknowledges that the future value of data often cannot be predicted at the time of collection, making preservation of raw data in its complete form a strategic imperative. By maintaining this comprehensive repository, organizations create a single source of truth that can support diverse analytical needs across departments and use cases without requiring redundant data collection or storage systems. This centralization simplifies governance while maximizing the potential utility of organizational information assets throughout their lifecycle.

## A. STRATEGIC BENEFITS OF DATA LAKE IMPLEMENTATION

The implementation of data lakes delivers numerous strategic advantages that extend beyond mere technical capabilities to transform how organizations derive value from their data. At the most fundamental level, data lakes democratize access to organizational information, enabling diverse user groups—from business analysts to data scientists—to leverage the same underlying data assets for their specific analytical needs. This accessibility drives innovation by allowing exploration of previously untested hypotheses and relationships within the data without requiring predefined schemas or complex data preparation workflows. The cost-effectiveness of data lake storage compared to traditional data warehousing solutions creates financial efficiency, particularly for organizations managing petabyte-scale information repositories. Modern advanced analytics applications, including machine learning algorithms that require access to vast amounts

of training data in various formats, find their ideal foundation in data lakes. These systems provide data scientists with unprocessed views of information, preserving nuances and anomalies that might be lost in heavily transformed datasets but could contain valuable signals for predictive modeling. As organizations increasingly compete on their ability to derive actionable insights from information, data lakes have become essential infrastructure components that support agile, data-driven decision making across operational and strategic levels.

## A. ARCHITECTURAL COMPONENTS OF ENTERPRISE DATA LAKES

The architecture of enterprise-grade data lakes represents a sophisticated balance between flexibility and governance, incorporating multiple layers that work in concert to deliver reliable data services. At the foundation lies the storage layer, which has traditionally leveraged Hadoop Distributed File System (HDFS) but increasingly incorporates cloud-native object storage solutions like Amazon S3, Azure Data Lake Storage, or Google Cloud Storage. This storage layer must support both schema-on-read approaches, where structure is imposed during data retrieval, and schema-on-write methodologies for use cases requiring more immediate data standardization. Above the storage foundation, data processing frameworks provide the computational engines that transform, aggregate, and analyze information—ranging from batch processing systems like Apache Spark to stream processing tools like Apache Flink that handle real-time data flows. Data cataloging and metadata management systems create searchable inventories of available datasets, documenting their origins, quality characteristics, and usage patterns. Security and governance layers implement access controls, encryption, and audit capabilities that ensure compliance with regulatory requirements while protecting sensitive information. Finally, the access layer provides interfaces for various user constituencies, from SQL query engines that serve business analysts to notebook environments supporting data scientists' exploratory work. These architectural components must work harmoniously to deliver a system that balances the flexibility needed for discovery with the controls required for enterprise data management.

## B. OPERATIONAL CHALLENGES AND IMPLEMENTATION CONSIDERATIONS

Despite their compelling advantages, data lakes present significant operational challenges that organizations must address to avoid creating unmanageable "data swamps." Data governance emerges as perhaps the most crucial consideration, requiring clear policies for data retention, quality management, security classification, and lifecycle management. Without effective governance, data lakes can quickly become unnavigable repositories of questionable information. Performance optimization presents another challenge, as the diverse workloads running against data lakes—from interactive queries to resource-intensive machine learning training—must coexist without mutual interference. Organizations must implement workload management strategies that include data tiering, where information is automatically moved between storage tiers based on access patterns and performance requirements. Integration with existing enterprise systems constitutes a third challenge area, requiring carefully designed data ingestion pipelines that maintain lineage tracking while accommodating diverse source systems. Skill requirements represent yet another consideration, as data lakes demand expertise spanning traditional data

warehouse administration, big data technologies, and cloud infrastructure management. Organizations implementing data lakes must therefore develop comprehensive transition strategies that address not only the technical architecture but also the operational processes and team capabilities required to derive sustainable value from these complex systems. With thoughtful implementation and ongoing management, data lakes can evolve into invaluable organizational assets that provide the foundation for data-driven transformation.

# IV. BLOCK CHAIN

## A. BUILDING BLOCKS OF BLOCK CHAIN

### A. SHARED LEDGER

The shared ledger forms the foundation of blockchain technology, serving as a distributed database that maintains identical copies across all network participants. Unlike traditional centralized databases, this ledger exists simultaneously across multiple locations, ensuring that all participants have access to the same information. Each transaction recorded on this ledger becomes permanent and transparent to all authorized participants, creating a single source of truth that eliminates discrepancies between different parties' records. The distributed nature of this ledger provides inherent redundancy, as the system continues functioning even if individual nodes fail.

### B. CONSENSUS MECHANISM

Consensus mechanisms enable network participants to agree on the validity of transactions without requiring a central authority. These protocols establish trust in a decentralized environment by providing rules for verifying transactions and adding new blocks to the chain. Different blockchain implementations employ various consensus approaches—including Proof of Work, Proof of Stake, and Delegated Proof of Stake—each balancing security, speed, and energy efficiency. The consensus mechanism prevents double-spending and ensures that only legitimate transactions are recorded on the blockchain, maintaining the integrity of the entire system.

### C. CRYPTOGRAPHY

Cryptographic techniques secure blockchain systems at multiple levels, protecting both transaction data and user identities. Public-private key pairs provide digital signatures that authenticate transaction sources while maintaining pseudonymity. Cryptographic hash functions create fixed-length outputs from transaction data, linking blocks together in a way that makes tampering immediately apparent. Each block contains the hash of the previous block, creating a chain where altering any single block would require changing all subsequent blocks—an increasingly difficult task as the chain grows longer. These cryptographic foundations establish the immutability that makes blockchain records trustworthy.

### d. SMART CONTRACTS

Smart contracts extend blockchain functionality beyond simple data storage by embedding self-executing code directly on the blockchain. These digital agreements automatically execute predefined actions when triggering conditions are met, without requiring intermediary involvement. Smart contracts enable complex business logic to operate in a trustless environment, supporting applications from automated insurance payouts to decentralized exchanges. By

eliminating manual contract enforcement, these programs reduce costs, increase efficiency, and minimize the potential for disputes between parties.

.

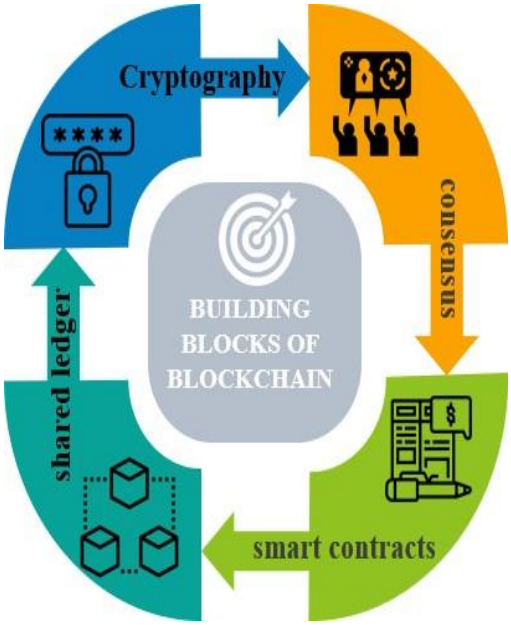


**Figure 1: Building blocks of blockchain**

## B. WORKING OF BLOCK CHAIN

Blockchain operates through a sequence of processes that maintain a secure, decentralized transaction record. When a user initiates a transaction, it is broadcast to all nodes in the peer-to-peer network. These participating nodes validate the transaction using predefined rules, verifying digital signatures and ensuring the sender has sufficient resources.

Valid transactions are collected into a block, which includes a cryptographic hash of the previous block, creating an unbreakable chain. To add this new block to the blockchain, a node must solve a complex computational challenge determined by the consensus mechanism (such as Proof of Work or Proof of Stake). This process, often called mining in Proof of Work systems, requires significant computational resources but ensures network security.

Once a solution is found, the new block is broadcast to the network. Other nodes verify the solution's correctness and, upon confirmation, add the block to their local copy of the blockchain. This distributed verification process ensures that all participants maintain identical ledger copies without requiring a central authority.

Each new block becomes permanently linked to all previous blocks through cryptographic hashes, making the record tamper-evident—any change to historical data would require altering all subsequent blocks, a task that becomes increasingly impossible as the chain grows. This immutability, combined with the distributed consensus mechanism, creates a trustworthy system where transactions, once recorded, cannot be modified or deleted, providing a transparent and secure foundation for digital interactions.

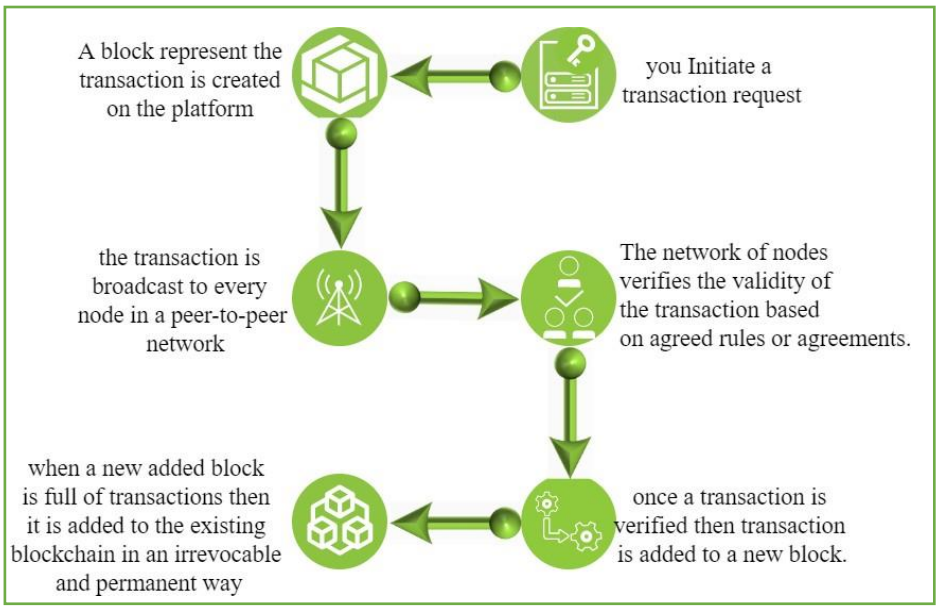


**Figure 2 : Working on blockchain**

# V. IMPLEMENTATION AND METHOD

## A. TECHNICAL ARCHITECTURE

The proposed technique utilizes MATLAB as the core application platform, featuring a comprehensive single-page application with multiple integrated dashboards. This design enables efficient communication between senders and receivers of sensitive healthcare information, providing a unified interface for all data exchange operations.

## B. CLOUD INTEGRATION

A cloud server deployed on the MongoDB Cloud platform forms the backbone of the data management system. The implementation incorporates Redis database technology within the cloud environment, creating a robust infrastructure for data operations. This cloud-based approach offers scalability advantages essential for handling healthcare data volumes.

## C. DATA MANAGEMENT PROCESS

The system implements a two-step process where communication occurs through the MATLAB application interface, followed by secure storage and retrieval operations via the cloud database. This architecture enables efficient data management while maintaining the security properties required for sensitive healthcare information exchange.

## D. BLOCKCHAIN-ENABLED SECURITY

The underlying blockchain technology ensures non-repudiation and fair exchange without requiring trusted third parties. Each transaction between healthcare entities is cryptographically secured and immutably recorded, creating an auditable trail that maintains data integrity throughout the exchange process.

### E. AI ENHANCEMENT LAYER

AI algorithms integrated within this framework optimize data processing, detect potential security threats, and prioritize information presentation. This intelligence layer improves system performance while providing advanced analytical capabilities that support clinical decision-making and research applications.

## VI. Basic Experiment

### EVALUATION MATRICES

The proposed blockchain-AI healthcare system is evaluated using standard security and performance metrics as outlined in Table 1.1. These metrics provide a comprehensive assessment of the system's effectiveness in protecting sensitive healthcare data.

### SECURITY CLASSIFICATION METRICS

- **True Positive (Detection Rate)**: Correctly identified unauthorized access attempts with appropriate alarms
- **False Positive**: System incorrectly flags legitimate access as unauthorized
- **True Negative**: System correctly allows legitimate access without raising alarms
- **False Negative**: System fails to detect actual unauthorized access attempts

### PERFORMANCE CALCULATION

The system's security performance is quantified using several derived metrics:

**Recall (Sensitivity)**

Measures the system's ability to detect all actual unauthorized access attempts:

Recall = TP / (TP + FN)

**Precision**

Measures the accuracy of positive predictions:

Precision = TP / (TP + FP)

**F1 Score**

Provides a balanced measure combining precision and recall:

F1 Score = 2 * (Precision * Recall) / (Precision + Recall)

### IMPLEMENTATION SIGNIFICANCE

These metrics enable objective evaluation of the blockchain-AI system's effectiveness in securing healthcare data exchanges. The balanced approach using both security detection measures (recall) and accuracy metrics (precision) ensures comprehensive performance assessment across different operational scenarios.

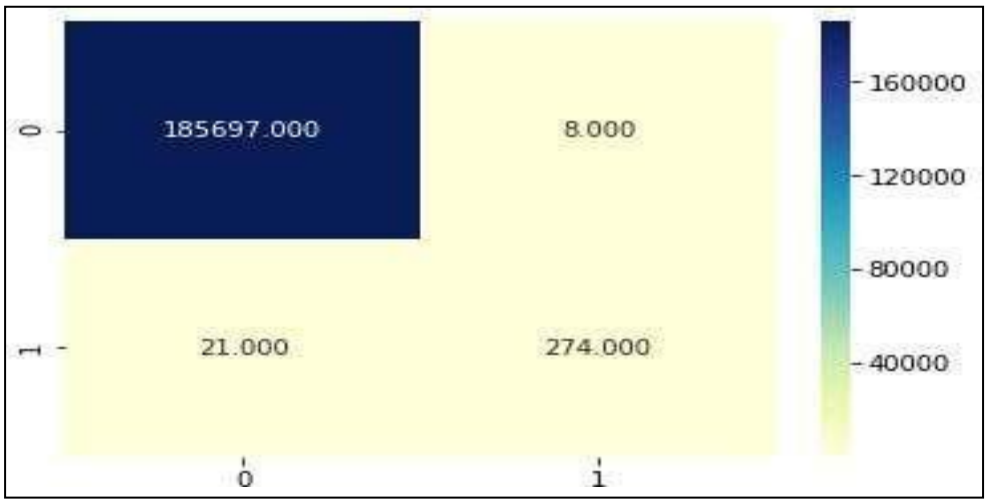


**Figure 3. The graph shows the Recall measure**

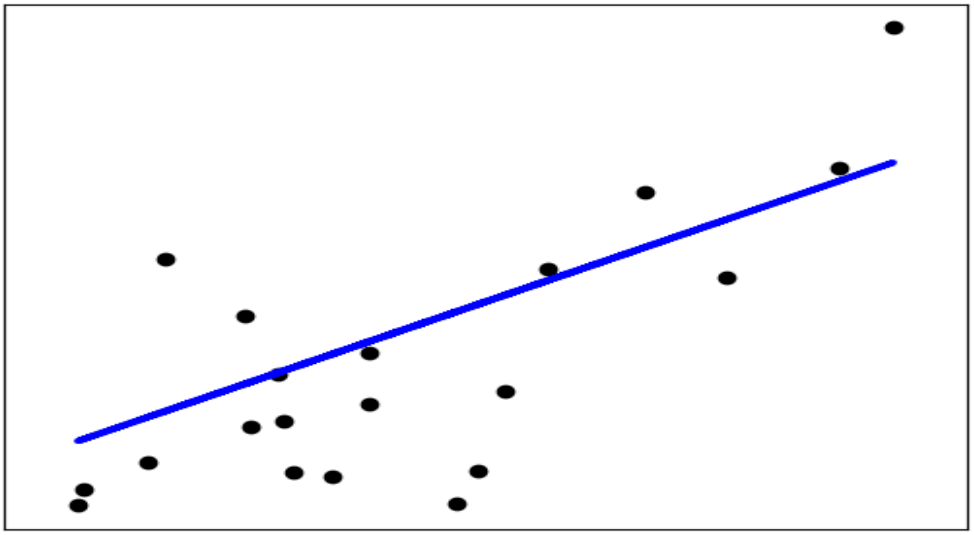

**Figure 4. Shows the graphical representation of the F1 score (dot) for ROC (line)**

Figure 1.4 shows the results obtained from the F1 score calculation processes. In this graph,the dot represents the F1 Score, and the cross line represents the ROC curve.

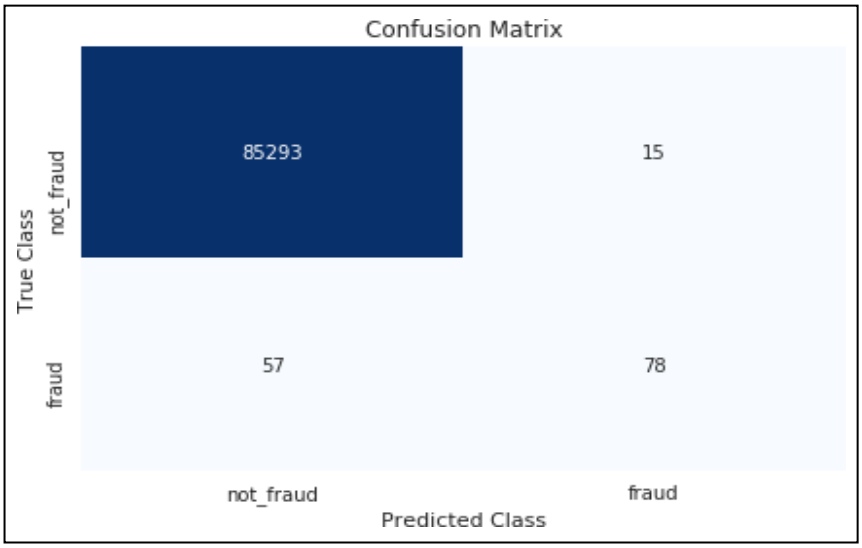


**Figure 5.** This figure shows the confusion Matrices

Figure 1.5 illustrates the graphical results of the proposed work by analyzing the predictionof fraudulent and non-fraudulent activities. Confusion matrices mainly fall into two classes, such as true class and predicted class. The proposed methodology is more effective than the existing ones.

## VI. PERFORMANCE ANALYSIS

### ENCRYPTION AND DECRYPTION EFFICIENCY

The proposed blockchain-AI healthcare data security model demonstrates superior performance in encryption and decryption processes compared to traditional cryptographic methods. As illustrated in Figure 1, the time required for both encryption and decryption operations is significantly lower than existing approaches.

Key observations from the encryption/decryption time analysis:

- The proposed model consistently outperforms RSA, ECC, and DH cryptographic methods
- Faster encryption enables more efficient secure data storage in the Data Lake
- Reduced decryption time improves data retrieval performance for healthcare applications

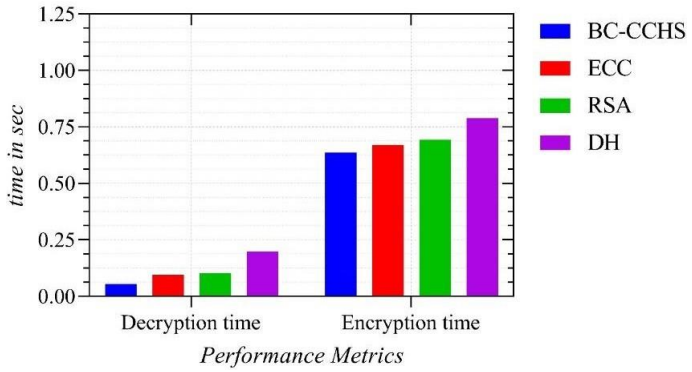


**Figure 6: Encryption And Decryption Efficiency**

## THROUGHPUT PERFORMANCE

The system achieves exceptional throughput metrics, indicating efficient data processing capabilities:

- Maximum throughput: 0.9861
- Minimum throughput: 0.7399

Comparative throughput analysis with existing methods:

- ECC: 0.95 (max) / 0.61 (min)
- RSA: 0.91 (max) / 0.53 (min)

The consistently higher throughput values demonstrate the proposed system's superior efficiency in handling healthcare data transactions.

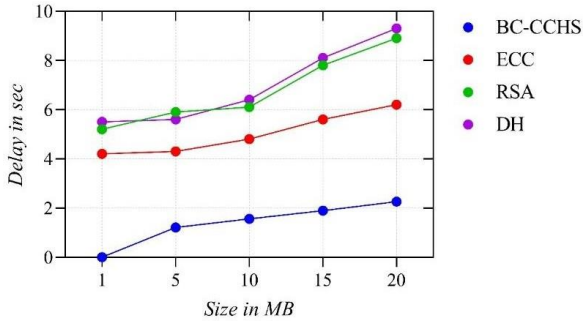


**Figure 7: Delay**

## DELAY AND LATENCY ANALYSIS

Figure 7 presents delay measurement comparisons between the proposed approach and existing methods. The results indicate reduced delay in data transmission and processing, which is critical for time-sensitive healthcare applications.

Figure 8 provides a comprehensive view of system performance through three key metrics:

- Transaction commit time
- Latency across different peer configurations
- Throughput at varying transaction rates

The latency analysis shows measurements from 0-60 seconds (Y-axis) against transaction rates in TPS (X-axis), demonstrating how the system performs under different organizational configurations with varying numbers of peers.These performance metrics collectively validate the efficiency and effectiveness of the proposed blockchain-AI integration for securing healthcare data exchanges.

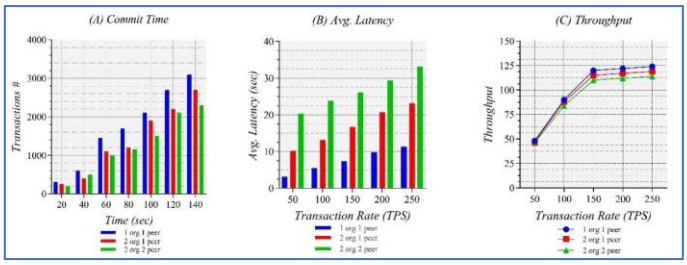


**Figure 8: Comprehensive View of System Performance**

## VII. CONCLUSION

The integration of blockchain technology and artificial intelligence presents a transformative approach to healthcare data security and management. This research demonstrates that the proposed system successfully addresses key challenges in healthcare information exchange without relying on trusted third parties. Performance analysis confirms the superiority of the proposed method over traditional cryptographic techniques like RSA, ECC, and DH across critical metrics including encryption/decryption time, throughput, and latency. The system achieves maximum throughput of 0.9861 while maintaining lower operational delays, making it suitable for time-sensitive healthcare applications. The MATLAB-based implementation with MongoDB Cloud and Redis database integration provides a robust framework for secure healthcare data exchange. The blockchain foundation ensures non-repudiation and immutability of records, while AI components enhance security through anomaly detection and intelligent data processing. This research contributes significantly to addressing the growing need for secure, efficient exchange of sensitive patient information across healthcare organizations. The proposed methodology establishes a foundation for future healthcare information systems that maintain data integrity and privacy while enabling authorized access for improved patient care and research applications. Further research directions may include optimizing the system for specific healthcare workflows, enhancing the AI capabilities for predictive analytics, and exploring additional consensus mechanisms to further improve performance in large-scale healthcare networks.

## VIII. FUTURE SCOPE

The integration of blockchain and AI technologies in healthcare information systems represents just the beginning of a transformative journey with extensive future potential. Several promising research directions emerge from this work, including the development of specialized consensus algorithms optimized for healthcare data that balance performance needs with clinical time-sensitivity requirements. Enhanced scalability solutions will be crucial as healthcare systems generate exponentially increasing volumes of data, potentially through layer-2 protocols or sharding techniques specifically designed for medical record management. Advanced privacy-preserving computation methods such as zero-knowledge proofs and homomorphic encryption could further strengthen patient data protection while still enabling valuable analytics. The system could evolve to incorporate interoperability standards that allow seamless communication between disparate healthcare blockchain networks across organizational and national boundaries. Integration with emerging technologies like Internet of Medical Things (IoMT) devices opens possibilities for real-time patient monitoring with blockchain-secured data transmission. Smart contracts could be extended to automate complex healthcare processes including insurance claims processing, clinical trial management, and supply chain verification for pharmaceuticals. As quantum computing advances, implementing quantum-resistant cryptographic methods will become essential to maintain long-term security of blockchain-stored health records. Perhaps most significantly, the expansion of patient-controlled data access mechanisms could revolutionize the healthcare data economy, potentially creating new models where individuals can selectively monetize their anonymized health data for research purposes while maintaining granular control over their information.

## IX. REFERENCES


1. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *2nd International Conference on Open and Big Data (OBD)*, 25-30.
2. Beam, A. L., & Kohane, I. S. (2018). Big data and machine learning in healthcare. *JAMA*, 319(13), 1317-1318.
3. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Ethereum White Paper*, 3(37), 2-1.
4. Chen, M., Hao, Y., Hwang, K., Wang, L., & Wang, L. (2017). Disease prediction by machine learning over big data from healthcare communities. *IEEE Access*, 5, 8869-8879.
5. Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. *Future Healthcare Journal*, 6(2), 94-98.
6. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. *Italian Conference on Cyber Security*.

7. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. *AMIA Annual Symposium Proceedings*, 650-659.
8. Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. *Nature*, 542(7639), 115-118.
9. Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal*, 16, 224-230.
10. Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, 3(2), 99-111.
11. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, 134, 104040.
12. Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 9(4), e1312.
13. Jensen, P. B., Jensen, L. J., & Brunak, S. (2012). Mining electronic health records: Towards better research applications and clinical care. *Nature Reviews Genetics*, 13(6), 395-405.
14. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211-1220.
15. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
16. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 1-3.
17. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*.
18. Rajput, A. R., Li, Q., Ahvanooey, M. T., & Masood, I. (2019). EACMS: Emergency access control management system for personal health record based on blockchain. *IEEE Access*, 7, 84304-84317.
19. Topol, E. J. (2019). High-performance medicine: The convergence of human and artificial intelligence. *Nature Medicine*, 25(1), 44-56.
20. Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing blockchains for efficient health care: Systematic review. *Journal of Medical Internet Research*, 21(2), e12439.
21. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5, 14757-14767.
22. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, 40(10), 218.

23. V. Panwar and D. S. K. Jain, “Blockchain Integrated Healthcare Wireless Body Area Network for Security Enhancement,” Smart Moves J. Ijoscience, pp. 23–27, Oct. 2021,doi: 10.24113/ijoscience.v7i10.434.
24. S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, “CoviChain: A Blockchain Based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems During Pandemic Outbreaks,” SN Comput. Sci., vol. 2, no. 5, p. 346, Jun. 2021,doi: 10.1007/s42979-021-00746-x.
25. S. A. El Rahman and A. S. Alluhaidan, “Blockchain technology and IoT-edge framework for sharing healthcare services,” Soft Comput., vol. 25, no. 21, pp. 13753–13777, Jul. 2021, doi: 10.1007/s00500-021-06041-4.
26. J. Ow, “The future of healthcare in Singapore. How an integrated use of A.I., Internet-of- Medical things (IoMT), Blockchain-based technologies, and Cloud-computing-based Medtech and Digital Health solutions will radically address medical data integrity concerns.,” SSRN Electron. J., 2021, doi: 10.2139/ssrn.3965116.
27. A. Giordanengo, “Possible usages of smart contracts (blockchain) in healthcare and whyno one is using them,” Stud. Health Technol. Inform., vol. 264, pp. 596–600, Aug. 2019,doi: 10.3233/SHTI190292.
28. S. Aich, S. Tripathy, M. Il Joo, and H. C. Kim, “Critical dimensions of blockchain technology implementation in the healthcare industry: An integrated systems management approach,” Sustain., vol. 13, no. 9, pp. 5269--, May 2021, doi: 10.3390/su13095269.
29. J. Peral, E. Gallego, D. Gil, M. Tanniru, and P. Khambekar, “Using visualization to build transparency in a healthcare blockchain application,” Sustain., vol. 12, no. 17, pp. 6768 , Aug. 2020, doi: 10.3390/SU12176768.
30. R. Adlam and B. Haskins, “Applying Blockchain Technology to Security-Related Aspects of Electronic Healthcare Record Infrastructure,” African J. Inf. Commun., vol.28, no. 28, pp. 1–28, Dec. 2021, doi: 10.23962/10539/32211.
31. Adler-Milstein, J., & Jha, A. K. (2017). HITECH Act drove large gains in hospital electronic health record adoption. *Health Affairs*, 36(8), 1416-1422.
32. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, 7(2), 56.
33. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2), 1676-1717.