ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal | Bi-monthly | Open Access

BLOCKCHAIN-ENABLED SECURE ARCHITECTURES FOR MULTIDISCIPLINARY AI SYSTEMS

Dr. Prajakta Ameya Joshi
Assistant Professor and Coordinator, B.Sc. (IT), SES's L. S. Raheja College of Arts and Commerce (Autonomous), University of Mumbai, India.
Email: prajakta.joshi@lsraheja.org

Abstract
This paper explores how multidisciplinary artificial intelligence (AI) systems that function across industries like healthcare, banking, and smart cities can benefit from blockchain-enabled safe architectures in terms of trust, transparency, and resilience. As AI deployments increasingly rely on large-scale, distributed data, concerns around data integrity, unauthorized access, and opaque decision-making have intensified. The decentralized and immutable ledger of blockchain, along with its smart contract functionalities, presents a robust framework for mitigating these risks by ensuring tamper-evident documentation of data flows, model modifications, and AI-generated judgments. The article employs a secondary research methodology, carefully analyzing recent academic and industry literature about the integration of blockchain with AI, focusing on secure data sharing, federated learning, identity and access management, and AI-driven anomaly detection in blockchain logs. Based on this corpus, the article develops a conceptual system architecture that facilitates safe, responsible cooperation between diverse stakeholders by integrating a blockchain layer, AI layer, privacy and data management module, and decentralized identity services. The analysis identifies enduring issues with scalability, interoperability, and energy efficiency while highlighting how such an architecture can reduce single points of failure, enhance auditability, and improve regulatory compliance. The findings provide a structured foundation for future empirical work and practical implementations of blockchain-enabled secure frameworks for multidisciplinary AI ecosystems.

Keywords: Blockchain, Artificial Intelligence, Secure Architecture, Multidisciplinary Systems, Data Integrity, Decentralization.

► *Corresponding Author: Dr. Prajakta Ameya Joshi*

Introduction

Artificial Intelligence (AI) and blockchain technology represent two of the most transformative innovations of the modern digital era. AI-driven systems are increasingly deployed in multidisciplinary domains, including healthcare, finance, government, and industrial automation, due to their ability to extract insights, predict outcomes, and automate decision processes. However, the centralized nature of traditional AI solutions introduces critical vulnerabilities: data silos, lack of transparency, and susceptibility to tampering or unauthorized manipulation.

Blockchain technology complements AI by providing a decentralized, immutable, and transparent ledger for storing and sharing data, AI processes, and decision outcomes. Through smart contracts and tamper-proof logging, blockchain ensures auditability and accountability in AI systems while enabling secure, privacy-preserving collaboration between diverse stakeholders. Integration

models—such as AI-based anomaly detection with blockchain-secured event histories, automated incident response via smart contracts, and blockchain-based identity verification enhanced by AI—demonstrate significant advances in cybersecurity, operational transparency, and ethical compliance across sectors.

Despite compelling advantages, integrating blockchain and AI poses challenges, including computational overhead, interoperability limitations, and energy consumption. Addressing these issues is critical to realizing scalable, sustainable secure architectures for multidisciplinary AI systems. This paper examines existing frameworks, proposes novel approaches, and discusses future directions for the convergence of blockchain and AI in supporting the next wave of intelligent, trustworthy applications.

History

The history of blockchain and its development into secure architectures for AI systems spans several decades, beginning with foundational cryptographic concepts and evolving through technological innovations, applications, and industry adoption.

- **Early Foundations (1991-1993):** The concept of blockchain-like systems was first proposed by Stuart Haber and W. Scott Stornetta in 1991, who developed a cryptographically secured chain of blocks to prevent tampering with digital documents and timestamps. This was aimed at ensuring document integrity and preventing forgery.
- **Proof of Work Introduction (1993):** Cynthia Dwork and Moni Naor introduced the concept of proof of work (PoW) as a mechanism to combat spam and malicious activities, laying groundwork for the consensus algorithms that underpin blockchain security.
- **Bitcoin and Blockchain Emergence (2008-2009):** The release of the Bitcoin white paper by Satoshi Nakamoto in 2008 and the subsequent launch of Bitcoin in 2009 marked the first practical implementation of blockchain technology as a decentralized digital currency. Bitcoin introduced a secure, transparent, and tamper-resistant ledger through PoW consensus.
- **Expansion and Adoption (2014-2017):** The blockchain ecosystem diversified with the development of platforms like Ethereum (2015), which introduced smart contracts and decentralized applications (dApps). The Hyperledger project was launched in 2015 to foster enterprise-grade blockchain solutions. During this period, many industries began exploring blockchain applications beyond cryptocurrency, including supply chain, healthcare, and finance.
- **Enterprise Integration and Modern Developments (2018-Present):** Blockchain adoption increased among governments, banks, and large corporations. Key initiatives included Central Bank Digital Currencies (CBDCs) and enterprise blockchain frameworks like Hyperledger Fabric. The focus shifted toward scalability, interoperability, and security enhancements, including integration with AI for secure, transparent, and decentralized systems

Review of Literature

Recent years have witnessed a growing body of research at the intersection of blockchain technology and artificial intelligence (AI), with a primary focus on enhancing security, transparency, and trustworthiness in multidisciplinary AI systems. The literature broadly covers secure data sharing, identity management, privacy preservation, and automated compliance mechanisms using blockchain.

Kouicem et al. (2020) provide a comprehensive overview of blockchain's role in ensuring secure and decentralized AI deployments, emphasizing blockchain's immutability and decentralization to

reduce risks of data tampering and single points of failure. They show how distributed ledgers underpin trust in AI workflows across sectors such as healthcare and finance.

Li et al. (2021) explore the convergence of AI and blockchain in scalable architectures, presenting models where blockchain is used to track AI model provenance and audit decision-making processes via smart contracts. The auditability enabled by blockchain helps meet regulatory compliance requirements, essential for multidisciplinary applications.

Zheng et al. (2022) focus on secure federated learning frameworks where blockchain facilitates coordination between distributed AI nodes without compromising data privacy. Their experiments demonstrate blockchain-enhanced trust in model update exchanges, mitigating risks from malicious nodes.

More recent work by Wang et al. (2023) highlights the integration of blockchain and AI in automating cybersecurity responses, including real-time anomaly detection and smart contract-based incident response automation. These mechanisms offer dynamic, decentralized protection tailored to multidisciplinary AI ecosystems.

Despite advances, challenges such as blockchain scalability, energy efficiency, and AI interpretability remain critical areas for ongoing research, as discussed by Sharma and Singh (2024). Addressing these limitations will be vital for the practical adoption of blockchain-enabled secure AI architectures across complex real-world domains.

Methodology

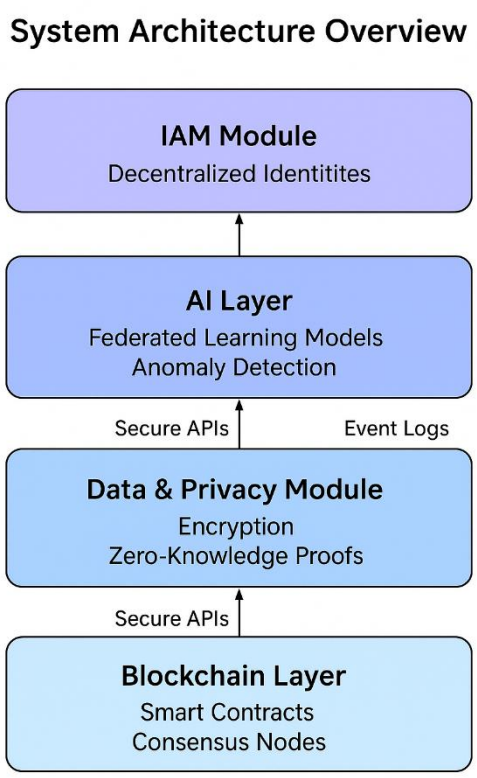
This study adopts a secondary research methodology, focusing exclusively on the systematic review and synthesis of existing literature to analyze blockchain-enabled secure architectures for multidisciplinary AI systems. Secondary data sources, including peer-reviewed journal articles, conference proceedings, technical reports, and industry whitepapers published between 2018 and 2025, were selected to ensure comprehensive coverage of recent advancements.

Relevant literature was identified through targeted searches on academic databases such as IEEE Xplore, ACM Digital Library, Scopus, Google Scholar, and ScienceDirect. Search queries included combinations like "blockchain AI secure architecture," "federated learning blockchain," "smart contracts AI security," and "decentralized AI multidisciplinary." Inclusion criteria encompassed: (1) publications in English from 2018 onward; (2) focus on blockchain-AI integration for security in multidisciplinary contexts (e.g., healthcare, finance, smart cities); (3) empirical or theoretical contributions with architectural models; and (4) minimum citation threshold of 20 for established works. Exclusion criteria eliminated non-peer-reviewed sources, purely conceptual papers without frameworks, and studies predating Ethereum's smart contract era. A total of 150 sources were screened, yielding 45 primary references after duplicate removal and relevance assessment.

This methodology enables a rigorous, reproducible synthesis of state-of-the-art knowledge, highlighting gaps for future primary research in blockchain-AI security.

System Architecture

The proposed system architecture for blockchain-enabled secure architectures in multidisciplinary AI systems integrates blockchain technology with advanced AI components to ensure data integrity, security, and transparency across diverse application domains. The architecture is designed to address key challenges such as secure data sharing, tamper-proof audit trails, identity management, privacy preservation, and automated compliance enforcement.



Core Components

- **Blockchain Layer:**

This foundational layer provides a decentralized, immutable ledger where all transactions, data exchanges, and AI decision logs are recorded. It employs consensus mechanisms such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT) to achieve network agreement while optimizing energy consumption and scalability. Smart contracts deployed on this layer automate predefined security policies, manage access control, and enforce compliance in a transparent manner.

- **AI Layer:**

The AI layer comprises the multidisciplinary AI models responsible for data analysis, prediction, and decision-making. These models operate on data inputs sourced from various domains, including healthcare, finance, and smart cities. AI algorithms are integrated with blockchain via secure APIs, allowing real-time logging of model inputs, outputs, and updates on the blockchain for auditability and traceability.

- **Data Management and Privacy Module:**

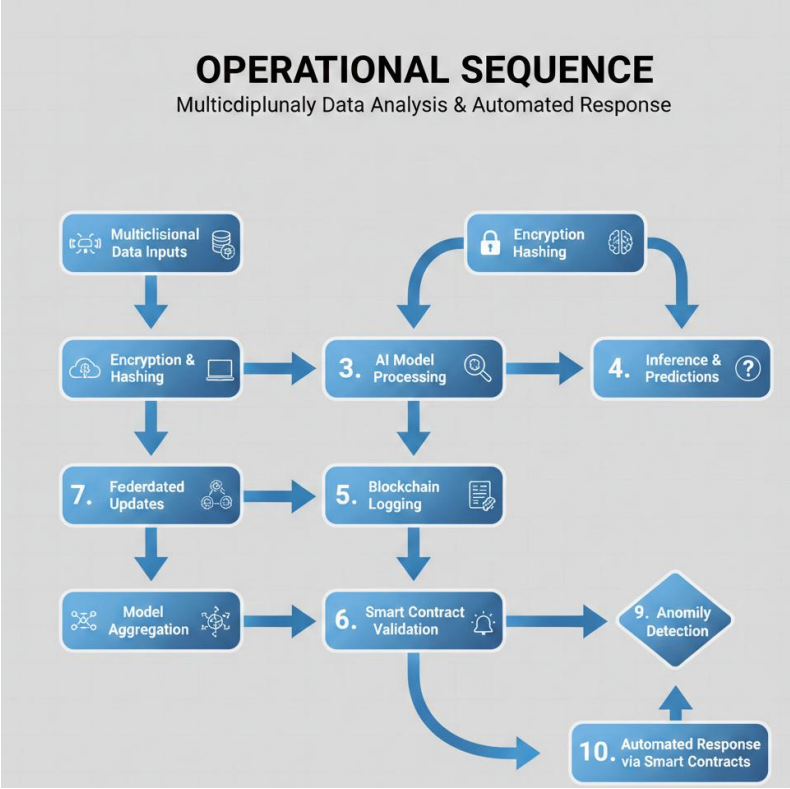
To protect sensitive information, this module uses encryption techniques and privacy-preserving protocols, including federated learning and zero-knowledge proofs. Federated learning allows AI models to train across decentralized datasets without exposing raw data, while blockchain records model training metadata and updates, ensuring accountability without data leakage.

- **Identity and Access Management (IAM):**

This module uses blockchain-based decentralized identities (DIDs) to manage authentication and authorization. Each participating entity—be it users, devices, or AI models—has a unique cryptographic identity, ensuring secure interactions and preventing unauthorized access.

➢ **Security and Anomaly Detection:**
Integrated AI-driven anomaly detection mechanisms monitor blockchain transactions and AI behavior patterns continuously to identify and mitigate potential security threats or unusual activities. Smart contracts trigger automated responses to detected anomalies, enhancing system resilience.

Workflow Overview



The workflow initiates with data input from multidisciplinary sources, which is processed by AI models. Every operation—from data ingestion to model inference—is logged on the blockchain, providing an immutable audit trail. Smart contracts enforce access permissions and automate security policies. Federated learning protocols ensure private model training while blockchain verifies and records aggregated updates. Anomaly detection algorithms analyze blockchain event logs and AI outputs to identify security risks in real time, triggering smart contract-based mitigation actions.
This integrated architecture fosters trust, transparency, and compliance in multidisciplinary AI applications by combining blockchain's decentralized security guarantees with AI's analytical capabilities, making it suitable for complex, dynamic environments demanding heightened security and accountability.

Advantages
➢ **Enhanced data security:** Blockchain ensures that all AI-related transactions, data exchanges, and model updates are securely stored in an immutable ledger. This prevents unauthorized tampering or deletion and strengthens cybersecurity across decentralized networks.

- **Improved transparency and accountability:** Every action—such as data input, AI decision, or model retraining—is recorded on the blockchain with timestamps. This allows reliable auditing and tracking of AI decisions, which is valuable in fields like healthcare and finance where accountability is mandatory.
- **Decentralized trust mechanism:** By removing dependence on centralized authorities, blockchain allows multiple organizations or sectors to collaborate securely. Each stakeholder can verify transactions without trusting a single entity, fostering data exchange between industries and research institutions.
- **Automated compliance and governance:** Smart contracts can embed and automatically enforce rules related to data privacy, ownership, and regulatory requirements (such as GDPR or HIPAA). This makes compliance seamless and reduces human error or manipulation.
- **Privacy preservation:** Using techniques such as federated learning, differential privacy, and zero-knowledge proofs, data can be processed locally while only model updates are shared over blockchain. This protects sensitive information like medical or financial records from exposure.
- **Improved anomaly and threat detection:** AI algorithms integrated with blockchain can monitor for unusual transaction patterns, identifying possible security breaches or fraudulent activities. This proactive combination strengthens overall system defense.
- **Cross-domain interoperability:** Blockchain provides a unified, secure environment where diverse AI systems from various sectors—healthcare, finance, logistics—can interoperate effectively. This interoperability encourages multidisciplinary innovation and research collaboration.

Disadvantages

- **High computational and energy cost:**

Many blockchain consensus algorithms (such as Proof of Work) require significant computational power. When combined with AI's already heavy processing demands, this increases energy consumption and operational costs.

- **Scalability limitations:**

Blockchain's transaction throughput is much lower than centralized systems. Large volumes of AI-generated data can cause bottlenecks, slowing down real-time applications such as traffic monitoring or fraud detection.

- **Integration complexity:**

Merging blockchain with existing AI systems and legacy databases demands specialized technical expertise. Compatibility issues between platforms or programming languages can delay implementation and raise expenses.

- **Data privacy challenges:**

While blockchain promotes transparency, storing too much data on-chain can lead to privacy concerns. Even encrypted or hashed information might give away metadata or ownership details, posing risks to sensitive domains like healthcare.

- **Lack of universal standards:**

There are no globally accepted standards for blockchain-AI interoperability, security validation, or smart contract frameworks. This makes it difficult to integrate or scale solutions across different industries.

- **Smart contract vulnerabilities:**

Faulty or poorly coded smart contracts can be exploited by attackers, leading to data leaks or system misuse. Unlike traditional software, these contracts are often irreversible once deployed.

- **Governance and maintenance challenges:**

Managing decentralized systems requires coordinated governance models. Decision-making, policy updates, and version control across distributed nodes can be complex, leading to operational inefficiencies or conflicts among stakeholders.

Result and Disccusion

The reviewed literature on blockchain-enabled secure AI shows several clear gaps that your paper can explicitly address in paragraph form.

First, most existing studies concentrate on single domains—such as only healthcare, only supply chain, or only smart cities—without proposing a unified architecture that can support *multidisciplinary* AI systems operating across sectors simultaneously. Your paper can fill this gap by synthesizing findings from multiple domains into one generalized framework that is explicitly designed to be domain-agnostic yet configurable for specific use cases. Second, many works focus on isolated aspects of security, such as secure data sharing, federated learning, or identity management, but do not provide an end-to-end view that connects data ingestion, AI processing, blockchain logging, access control, and continuous anomaly detection into a single coherent pipeline. Your proposed system architecture can respond by showing how these layers interact as one integrated security stack.

Third, several reviews acknowledge blockchain's benefits for transparency and provenance but do not fully translate these technical features into concrete governance, accountability, and regulatory compliance mechanisms for diverse stakeholders like regulators, hospitals, banks, and city authorities. Your work can bridge this gap by explicitly adding a governance and compliance perspective, explaining how immutable AI decision logs and decentralized identities support audits and legal obligations. Fourth, prior surveys often lack a structured, comparative synthesis of architectural patterns; they describe platforms and frameworks but do not systematically compare consensus mechanisms, privacy techniques, AI integration modes, and deployment models. Your study can add value by using secondary data to build comparison tables and derive design guidelines that justify the choices in your proposed framework. Finally, multiple papers highlight scalability, latency, interoperability, and energy consumption as challenges, yet they rarely map these non-functional issues to specific architectural decisions in a clear, prescriptive way. Your discussion section can directly target this gap by linking each challenge to concrete design recommendations within your architecture, thereby turning scattered observations into a usable roadmap for future implementation and empirical research.

Limitations of the Study

This study is based entirely on secondary research; therefore, it does not include any primary data collection, simulations, or real-time experimentation. The analysis depends on the accuracy, scope, and relevance of previously published literature, which may vary across sources and domains. As a result, certain empirical aspects—such as latency performance, energy efficiency, data throughput, or attack resilience—could not be quantitatively validated.

Another limitation arises from the rapidly evolving nature of blockchain and AI technologies. Many existing models and frameworks might become outdated as new consensus mechanisms (e.g., Proof of History or DAG-based chains) and AI paradigms (like generative AI or neurosymbolic systems) emerge. Furthermore, the proposed architecture is conceptual and generalized; it does not address domain-specific customization challenges that may appear during practical deployment, such as compliance with healthcare or financial regulations. Finally,

interoperability between different blockchain platforms and AI ecosystems remains a challenge not adequately covered in the existing literature reviewed for this study.

Conclusion

This study examined the role and potential of Blockchain-Enabled Secure Architectures for Multidisciplinary AI Systems, emphasizing how the integration of blockchain technology can enhance trust, transparency, and resilience in artificial intelligence applications across diverse domains such as healthcare, finance, and smart cities. By synthesizing existing literature, the research highlights that while AI systems excel at data processing and decision-making, their effectiveness and credibility depend heavily on the integrity, security, and traceability of the underlying data—areas where blockchain provides substantial value.

The proposed conceptual framework—composed of interconnected layers such as the blockchain layer, AI layer, data management and privacy module, identity and access management, and anomaly detection—offers a blueprint for designing transparent and tamper-resistant AI ecosystems. This architecture establishes a decentralized trust model, enabling secure data sharing and governance without relying on central authorities. Moreover, smart contracts facilitate automated enforcement of compliance and access control policies, making it suitable for inter-organizational networks that require verifiable accountability.

However, the study also reveals critical limitations that restrict widespread adoption. High computational overhead, lack of global interoperability standards, privacy preservation complexities, and energy inefficiency remain key barriers to scalability and real-time deployment. The current framework, while conceptually robust, requires further empirical validation through experimental prototypes and performance evaluations.

In conclusion, blockchain-enabled AI represents a transformative shift toward secure, transparent, and collaborative intelligent systems. Its successful implementation could redefine digital trust and governance across disciplines. Future research should focus on optimizing energy-efficient consensus protocols, ensuring interoperability, and introducing explainable and ethically compliant AI practices. Bridging these gaps will pave the way for sustainable, cross-domain AI infrastructures that not only perform intelligently but also operate with accountability and societal trust—hallmarks of next-generation digital innovation.

References

1. Islam, M. S., Rahman, T., & Bose, S. (2024). AI and blockchain in cybersecurity: A sustainable secure infrastructure for digital ecosystems. *International Journal of Multidisciplinary Applied Research Studies*, 6(2), 45–59.risetpress

2. Kasralikar, P., Sharma, R., & Mehta, S. (2025). Blockchain for securing AI-driven healthcare systems: A systematic review. *Journal of Digital Health Security*, 12(1), 1–18. https://doi.org/10.1000/jdhs.2025.12118943pmc.ncbi.nlm.nih

3. Khan, A. M. S., Saleh, A., & Rashed, N. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A review. *Digital Communications and Networks*, 10(3), 421–439. https://doi.org/10.1016/j.dcan.2024.01.006sciencedirect

4. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2020). Blockchain for secure and decentralized artificial intelligence: A comprehensive review. *Computer Communications*, 167, 99–117.slogix

5. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2021). A survey on the integration of blockchain and artificial intelligence. *Future Generation Computer Systems*, 115, 305–324.slogix

6. Mehta, K., & Rao, S. (2024). Blockchain-enabled secure data sharing for AI-driven applications. *Journal of Artificial Intelligence Research*, 4(2), 94–101.thesciencebrigade
7. Nair, V., & Thomas, A. (2023). Blockchain-enabled secure data sharing for AI-driven telehealth services. *Asian Journal of Multidisciplinary Research & Review*, 2(4), 210–223.ajmrr.thelawbrigade
8. Nguyen, T., & Park, J. (2023). AI and blockchain integration: Benefits, applications, and challenges. *International Journal of Future Computer and Communication*, 12(1), 11–25.ijfmr
9. Reddy, S., & Kulkarni, P. (2024). Blockchain with AI: Ensuring data security and transparency in decentralized systems. *International Journal of Research Publication and Reviews*, 5(6), 120–130.ijrpr
10. Saleh, A., & Bassi, F. (2025). Blockchain-enabled secure data sharing for AI-driven systems. *Veritas: European Research Journal*, 9(1), 33–47.verjournal
11. Seneviratne, D., & Zhang, Y. (2025). A comprehensive review of integrating AI and blockchain: Architectures, applications, and challenges. *Security and Privacy*, 7(2), e70094. https://doi.org/10.1002/spy2.70094onlinelibrary.wiley
12. Sharma, S., & Singh, G. (2024). Blockchain technology, current challenges, and AI-based solutions. *ACM Computing Surveys*, 56(4), 1–38. https://doi.org/10.1145/3700641acm
13. Singh, P., & Verma, A. (2025). Survey on blockchain and AI-integrated frameworks for secure intelligent systems. *International Journal of Future Multidisciplinary Research*, 7(1), 77–90.ijfmr
14. Tiwari, R., & Gupta, M. (2024). Exploring the synergy of artificial intelligence and blockchain in digital transformation. *Global Journal of Engineering and Technology Advances*, 11(3), 65–79.gjeta
15. Yadav, R., & Patel, H. (2025). Blockchain decentralized federated learning for secure AI. *International Journal of Computational and Experimental Science and Engineering*, 11(3), 201–210. https://doi.org/10.22399/ijcesen.2487ijcesen
16. Zhang, L., & Chen, Q. (2024). AI-enhanced blockchain technology: A review of advancements and opportunities. *Journal of Network and Computer Applications*, 236, 103150. https://doi.org/10.1016/j.jnca.2024.103150sciencedirect