EuroVantage
Journal of Artificial Intelligence

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

Blockchain-Supported Intelligent Systems for Privacy-Preserving Data Analytics

Emma Stacy

University of Cambridge, UK

Corresponding Author: iemmastacy@nuzm.ee

Abstract

The rapid growth of intelligent systems and data-driven technologies has increased the demand for secure and privacy-preserving data analytics. Organizations increasingly rely on machine learning and artificial intelligence to extract insights from massive datasets, yet the sensitive nature of modern data—such as healthcare records, financial transactions, and personal behavioral information—creates significant privacy challenges. Traditional centralized analytics frameworks often require data sharing among multiple entities, which increases risks of unauthorized access, data leakage, and privacy violations. Blockchain technology has emerged as a promising solution to these challenges due to its decentralized architecture, immutable ledger, and cryptographic security mechanisms. This research investigates a blockchain-supported intelligent system framework designed to enable privacy-preserving data analytics across distributed environments. The proposed architecture integrates blockchain infrastructure with advanced privacy-preserving techniques such as federated learning, homomorphic encryption, and differential privacy to allow collaborative analytics without exposing raw data. Blockchain acts as a secure coordination layer that records transactions, ensures data integrity, and enforces trust among participants.

Keywords: Blockchain, Privacy-Preserving Analytics, Intelligent Systems, Federated Learning, Secure Data Sharing, Distributed Machine Learning

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

I. Introduction

The exponential growth of digital data has transformed modern industries into highly data-driven ecosystems where intelligent systems continuously analyze large volumes of information. Artificial intelligence and machine learning technologies rely on data availability to train models, detect patterns, and make predictions [1]. However, the increasing dependence on data analytics raises serious concerns about privacy protection, data ownership, and secure data sharing across organizations. Sensitive data such as healthcare records, financial transactions, and personal behavioral data must be protected from unauthorized access while still enabling meaningful analytics.

Traditional data analytics architectures rely heavily on centralized data repositories where information from multiple sources is aggregated and processed. Although centralized infrastructures simplify analytics workflows, they create critical vulnerabilities including data breaches, insider threats, and misuse of personal information. These risks are further amplified in multi-organization environments where entities may not fully trust each other. As a result, organizations are often reluctant to share valuable datasets, limiting the potential benefits of collaborative analytics.

Blockchain technology introduces a decentralized paradigm that can address many of these challenges by eliminating reliance on centralized authorities. A blockchain network maintains a distributed ledger where transactions are verified through consensus mechanisms and stored immutably across multiple nodes [2]. This decentralized architecture enhances transparency, accountability, and data integrity, making blockchain an attractive solution for secure data exchange and collaboration.

Despite these advantages, blockchain alone does not guarantee privacy protection because public blockchain ledgers are inherently transparent. Without additional mechanisms, sensitive information stored on blockchain networks could potentially expose confidential data.

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

Consequently, privacy-preserving techniques must be integrated with blockchain infrastructures to ensure that analytical operations can be performed without revealing raw data.

Recent research has explored combining blockchain with cryptographic approaches such as zero-knowledge proofs, secure multiparty computation, and homomorphic encryption. These techniques enable computations to be performed on encrypted data or allow verification of information without disclosing underlying values [3]. By integrating these mechanisms with intelligent systems, it becomes possible to perform collaborative analytics while preserving privacy.

This paper proposes a blockchain-supported intelligent system framework designed to facilitate privacy-preserving data analytics across distributed environments [4]. The framework combines decentralized blockchain infrastructure with privacy-enhancing computation techniques and machine learning algorithms to enable secure collaborative analytics without exposing sensitive datasets.

II. Background and Related Work

Blockchain technology has rapidly evolved from its initial use in cryptocurrency systems into a broader infrastructure for secure distributed computing. The decentralized ledger mechanism ensures that all transactions are recorded in a tamper-resistant and verifiable manner. This property is particularly useful for applications requiring transparency and auditability, such as financial systems, healthcare data sharing, and supply chain management.

Researchers have increasingly explored the integration of blockchain with intelligent systems to enhance data trustworthiness and transparency. Intelligent systems rely heavily on accurate and trustworthy data to train machine learning models and make decisions [5]. Blockchain can serve as a trusted data management layer where datasets are securely registered and verified before being used for analytics tasks. This approach helps reduce data manipulation and ensures traceability of data sources.

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

Privacy-preserving techniques are essential components in blockchain-based analytics systems. Differential privacy is widely used to protect sensitive information by introducing controlled noise into datasets or analytical outputs. This method ensures that individual records cannot be identified while still allowing meaningful statistical analysis. Local differential privacy approaches further enhance protection by sanitizing data at the source before it is shared or processed.

Another widely adopted technique is homomorphic encryption, which enables computations to be performed directly on encrypted data without decrypting it [6]. This capability is particularly useful for distributed analytics scenarios where multiple parties wish to collaborate while keeping their data confidential. Secure multiparty computation similarly allows multiple participants to jointly compute analytical results without revealing their private inputs.

Federated learning has emerged as a promising paradigm for privacy-preserving machine learning. In this approach, machine learning models are trained collaboratively across multiple devices or organizations while keeping data locally stored. Only model updates are shared and aggregated, reducing the risk of sensitive data exposure. Integrating federated learning with blockchain networks can remove the need for centralized aggregation servers while improving trust and transparency in the training process [7].

Existing research demonstrates the potential of combining blockchain with privacy-preserving computation, but many solutions remain limited in scalability, efficiency, or real-world applicability. Some frameworks focus primarily on data storage security while neglecting analytical processes, whereas others emphasize machine learning privacy without addressing trust and coordination among participating entities. These limitations highlight the need for integrated architectures capable of supporting secure, decentralized, and privacy-preserving analytics.

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

III. Proposed Blockchain-Supported Intelligent System Framework

The proposed framework introduces a decentralized architecture designed to support privacy-preserving analytics across distributed organizations. The architecture consists of multiple layers including the blockchain network layer, the privacy-preserving computation layer, and the intelligent analytics layer. Each component plays a distinct role in ensuring data security, privacy protection, and analytical efficiency.

The blockchain layer functions as the trust infrastructure of the system. It records all data transactions, model updates, and analytical requests in an immutable ledger that is accessible to authorized participants. Smart contracts enforce access control policies and manage interactions between data providers, analytics nodes, and data consumers. By eliminating reliance on a central authority, the blockchain network ensures fairness and transparency in collaborative analytics processes.

The privacy-preserving computation layer integrates advanced cryptographic techniques that allow analytical tasks to be performed without exposing sensitive information. Homomorphic encryption enables encrypted datasets to be processed securely, while secure multiparty computation allows multiple organizations to jointly compute results without revealing individual data inputs. Differential privacy mechanisms further ensure that analytical outputs cannot be used to infer sensitive details about individual records.

The intelligent analytics layer incorporates machine learning algorithms and data mining techniques to extract meaningful insights from distributed datasets. Federated learning models are trained locally on participating nodes, allowing organizations to maintain control over their data while contributing to a shared global model. Blockchain records model updates and validation steps to ensure transparency and prevent malicious modifications.

The framework also incorporates decentralized storage mechanisms such as distributed file systems for managing large datasets. Instead of storing raw data directly on the blockchain—which would be inefficient and potentially expose sensitive information—the system stores

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

encrypted data off-chain while maintaining cryptographic references on-chain. This hybrid architecture improves scalability while preserving security.

Overall, the proposed system creates a secure ecosystem where organizations can collaborate on data analytics tasks without compromising privacy. By combining blockchain's decentralized trust model with advanced privacy-preserving computation techniques, the framework enables secure data sharing and collaborative intelligence across multiple stakeholders.

IV. Experimental Setup and Methodology

To evaluate the effectiveness of the proposed framework, a prototype system was implemented using an Ethereum-based blockchain environment. The blockchain network consisted of multiple distributed nodes representing different organizations participating in collaborative analytics tasks. Smart contracts were developed to manage authentication, data access permissions, and model update verification.

The experimental setup integrated federated learning mechanisms with blockchain infrastructure. Each participating node maintained a local dataset and trained machine learning models locally. Model updates were encrypted and transmitted to the blockchain network where they were validated and aggregated to form a global model. This approach ensured that raw data remained within local environments while still contributing to collaborative analytics.

The experimental dataset consisted of distributed healthcare and financial transaction records simulated across multiple nodes. Privacy-preserving techniques including differential privacy and homomorphic encryption were applied to ensure that individual records remained confidential during analysis. Encryption keys and access control policies were managed through blockchain-based smart contracts [8].

Performance metrics were defined to evaluate the system's effectiveness in terms of privacy protection, analytical accuracy, computational overhead, and network latency. Privacy protection was measured using differential privacy guarantees and resistance to inference attacks.

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

Analytical accuracy was evaluated by comparing the performance of federated models with centralized machine learning models trained on aggregated datasets.

The experiments were conducted over multiple training rounds to simulate real-world distributed learning scenarios. During each round, nodes trained local models, encrypted model parameters, and submitted updates to the blockchain network. Smart contracts validated the updates before aggregating them into the global model. This process ensured both transparency and accountability throughout the training workflow.

The evaluation environment included distributed computing nodes with varying computational capabilities to simulate heterogeneous real-world networks. The system was tested under different network sizes and dataset distributions to assess scalability and robustness.

V. Results and Discussion

The experimental results demonstrate that the proposed blockchain-supported intelligent system effectively enables privacy-preserving data analytics while maintaining strong analytical performance. The federated learning models trained within the framework achieved predictive accuracy comparable to centralized machine learning models, indicating that collaborative analytics can be performed without requiring direct data sharing.

Privacy protection was significantly enhanced through the integration of differential privacy and cryptographic techniques. The experiments confirmed that individual data records could not be reconstructed or inferred from model updates or analytical outputs. This demonstrates that privacy-preserving analytics can be achieved without compromising analytical quality.

The blockchain network successfully provided secure coordination and auditing capabilities for the distributed analytics process [9]. All model updates, training rounds, and validation steps were recorded immutably on the blockchain ledger, ensuring transparency and traceability. This property is particularly valuable for applications in regulated industries such as healthcare and finance where auditability is essential.

Pages: 17-25
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

However, the integration of blockchain infrastructure introduced certain computational and latency overheads. Transaction verification and consensus processes increased the time required for model update validation compared to purely centralized architectures. Despite this overhead, the overall performance remained within acceptable limits for distributed analytics applications.

Scalability experiments revealed that the system can support a growing number of participating nodes without significant degradation in analytical performance [10]. The use of off-chain storage and hybrid architectures helped reduce blockchain storage requirements while maintaining security. This design ensures that the framework can be applied to large-scale analytics environments involving multiple organizations.

Overall, the results highlight the potential of blockchain-supported intelligent systems to enable secure collaborative analytics across distributed environments. The combination of decentralized trust mechanisms and privacy-preserving computation techniques creates a powerful platform for secure data-driven innovation [11].

VI. Conclusion

Blockchain-supported intelligent systems provide a promising foundation for privacy-preserving data analytics in distributed environments where data confidentiality, trust, and transparency are critical requirements. This research proposed a decentralized framework that integrates blockchain infrastructure with privacy-preserving computation techniques and intelligent analytics models. The experimental evaluation demonstrated that the proposed architecture can enable collaborative analytics without exposing sensitive datasets while maintaining competitive analytical performance. By combining federated learning, differential privacy, cryptographic computation, and blockchain-based trust mechanisms, the framework ensures secure data sharing, auditability, and privacy protection across multiple organizations. Although challenges related to scalability and computational overhead remain, the results highlight the strong potential of blockchain-enabled intelligent systems to transform secure data analytics across sectors such as healthcare, finance, and smart infrastructure. Future research should focus on

optimizing consensus mechanisms, improving scalability, and developing standardized architectures to support large-scale deployment of privacy-preserving blockchain analytics systems.

REFERENCES:

[1] S. Khairnar, G. Bansod, and V. Dahiphale, "A light weight cryptographic solution for 6LoWPAN protocol stack," in *Science and Information Conference*, 2018: Springer, pp. 977-994.

[2] S. Khairnar, "EXPLORING CORPORATE CLOUD ADOPTION: A COMPREHENSIVE MULTI-FACTOR EVALUATION," *International Journal of Data Science and IoT Management System,* vol. 1, no. 3, pp. 35-50, 2022.

[3] T. Hagendorff, "Forbidden knowledge in machine learning reflections on the limits of research and publication," *Ai & Society,* vol. 36, no. 3, pp. 767-781, 2021.

[4] S. Khairnar, "AN ENERGY-AWARE SYMMETRIC CRYPTOGRAPHIC FRAMEWORK FOR SMART HOME IOT APPLICATIONS."

[5] C. C. K. Chan, V. Kumar, S. Delaney, and M. Gochoo, "Combating deepfakes: Multi-LSTM and blockchain as proof of authenticity for digital media," in *2020 IEEE/ITU International Conference on Artificial Intelligence for Good (AI4G)*, 2020: IEEE, pp. 55-62.

[6] J. Bateman, *Deepfakes and synthetic media in the financial system: Assessing threat scenarios*. Carnegie Endowment for International Peace., 2022.

[7] S. Khairnar "EDGE COMPUTING FOR IOT DEVICES: A COMPREHENSIVE FRAMEWORK FOR DISTRIBUTED DATA PROCESSING AND REALTIME ANALYTICS," *Journal of Integrated Research,* vol. 2, no. 1, 2021.

[8] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys (CSUR),* vol. 48, no. 3, pp. 1-39, 2015.

[9] F. Heiding, B. Schneier, A. Vishwanath, J. Bernstein, and P. S. Park, "Devising and detecting phishing: Large language models vs. smaller human models," *arXiv preprint arXiv:2308.12287,* 2023.

[10] A. Antinori, "Terrorism and deepfake: From hybrid warfare to post-truth warfare in a hybrid world," in *ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics*, 2019: Academic Conferences and publishing limited, p. 23.

[11] Y. Hu, F. Zou, J. Han, X. Sun, and Y. Wang, "Llm-tikg: Threat intelligence knowledge graph construction utilizing large language model," *Computers & Security,* vol. 145, p. 103999, 2024.