EuroVantage
Journal of Artificial Intelligence

Pages: 1-8
Volume-I, Issue-III, 2024
https://evjai.com/index.php/evjai

A Trust-Aware Intelligent Systems Framework for Secure Data Exchange Using Blockchain

Park Ji Hyun

Yonsei University, Seoul, South Korea

Corresponding Author: park.hyun@interviauniversity.com

Abstract

Secure data exchange has become a critical requirement for modern intelligent systems that operate across distributed and heterogeneous environments. As artificial intelligence applications increasingly rely on collaborative data sharing among organizations, devices, and platforms, ensuring trust, integrity, and privacy in the exchanged information becomes a fundamental challenge. Traditional centralized security mechanisms often fail to provide sufficient transparency and tamper resistance, especially when multiple stakeholders with varying trust levels are involved. Blockchain technology, with its decentralized ledger architecture and cryptographic validation mechanisms, offers a promising solution to address these issues. This research proposes a trust-aware intelligent systems framework that leverages blockchain technology to facilitate secure and reliable data exchange across distributed intelligent environments. The framework integrates trust evaluation models with blockchain-based distributed ledgers to ensure that data transactions are verified, immutable, and traceable.

Keywords: Blockchain, Intelligent Systems, Secure Data Exchange, Trust Management, Distributed Ledgers, Smart Contracts, Data Integrity, Cybersecurity

I. Introduction

The rapid advancement of intelligent systems has transformed how data is generated, processed, and shared across digital environments. Artificial intelligence-driven applications such as autonomous systems, smart healthcare platforms, and intelligent financial services rely heavily on continuous data exchange between multiple entities [1]. In many of these environments, organizations collaborate by sharing sensitive datasets, predictive models, or operational insights. However, the lack of reliable trust mechanisms often creates security risks, including data tampering, unauthorized access, and malicious manipulation of shared information [2].

Traditional data exchange architectures are largely based on centralized infrastructures where a single authority manages authentication and access control. Although such systems can enforce certain security policies, they often suffer from single points of failure and limited transparency. If the central authority is compromised, the entire system becomes vulnerable to attacks. Moreover, centralized systems often require participants to fully trust the governing authority, which is not always feasible in decentralized or multi-stakeholder environments.

Blockchain technology introduces a decentralized model that eliminates reliance on a single trusted authority. By maintaining a distributed ledger across multiple nodes, blockchain ensures that all transactions are cryptographically validated and permanently recorded [3]. This structure makes data manipulation extremely difficult because altering any stored information would require consensus across the network. As a result, blockchain provides a reliable mechanism for ensuring data integrity and transparency in distributed systems.

Despite the advantages of blockchain, many intelligent systems still face challenges related to trust evaluation among participating entities. Simply verifying a transaction on the blockchain does not guarantee that the data source itself is trustworthy. For example, an intelligent sensor could submit incorrect data that is cryptographically valid but semantically unreliable. Therefore, integrating trust-aware evaluation mechanisms into blockchain-enabled systems becomes essential.

This research proposes a trust-aware framework that combines intelligent trust computation models with blockchain-based verification mechanisms. The objective is to create a secure environment where intelligent systems can evaluate the credibility of data sources while ensuring that exchanged information remains immutable and verifiable. Such an approach enables secure collaboration among autonomous systems without requiring centralized control.

The rest of this paper presents the proposed framework, experimental evaluation, and analysis of results demonstrating how blockchain-enabled trust models can significantly improve the security and reliability of data exchange in intelligent systems.

II. Related Work

In recent years, researchers have explored various approaches to secure data exchange within intelligent systems. Many traditional solutions rely on encryption protocols, authentication mechanisms, and access control policies to protect sensitive information during transmission. While these techniques provide essential security layers, they often fail to address trust management in distributed environments where participants may not fully trust each other [4].

Several studies have investigated blockchain as a tool for improving data integrity and transparency in distributed computing systems. Blockchain-based frameworks allow organizations to record transactions in an immutable ledger, making it easier to track data origins and detect unauthorized modifications. These systems have been applied in areas such as supply chain management, healthcare data sharing, and financial services.

In intelligent systems research, blockchain has been increasingly used to support secure machine learning workflows. For example, blockchain-based architectures have been proposed for federated learning environments where multiple organizations collaboratively train AI models without sharing raw data. In these scenarios, blockchain ensures that model updates are verified and recorded in a tamper-proof ledger [5].

Another area of research focuses on trust management models for distributed networks. Trust evaluation mechanisms analyze the behavior, reliability, and historical interactions of entities to determine their credibility. These models often rely on reputation scores, behavioral analytics, and probabilistic trust metrics. Integrating such mechanisms into intelligent systems allows agents to make informed decisions about data sources.

However, most existing studies treat blockchain and trust management as separate components rather than integrating them into a unified framework. Blockchain ensures transaction immutability, while trust models assess participant credibility, but the interaction between these two components is rarely optimized. This separation limits the effectiveness of security architectures designed for complex intelligent ecosystems.

The proposed research addresses this limitation by embedding trust evaluation directly into a blockchain-enabled data exchange framework. By combining trust computation with distributed ledger validation, the system provides both data integrity and dynamic trust assessment, ensuring more reliable collaboration among intelligent agents.

III. Proposed Trust-Aware Framework

The proposed framework is designed to facilitate secure and trustworthy data exchange among intelligent systems operating in distributed environments. The architecture consists of multiple integrated components that collectively ensure secure communication, trust verification, and immutable data recording. These components include intelligent data acquisition modules, trust evaluation engines, blockchain validation layers, and secure data exchange protocols.

At the core of the framework lies the intelligent trust evaluation module, which continuously assesses the reliability of participating entities [6]. This module analyzes historical interactions, behavioral patterns, and transaction outcomes to compute trust scores for each participant. These trust scores influence whether an entity is permitted to share or receive data within the network.

Blockchain technology is used as the underlying infrastructure for recording data exchange transactions. Every interaction between participating entities is logged as a blockchain transaction, ensuring transparency and immutability. Once recorded in the distributed ledger, the transaction cannot be modified without consensus from the network nodes.

Smart contracts play a crucial role in automating security policies within the framework [7]. These programmable contracts enforce predefined rules for data exchange, including authentication requirements, trust thresholds, and access permissions. If an entity fails to meet the required trust level, the smart contract automatically blocks the transaction.

The framework also incorporates encryption mechanisms to ensure data confidentiality during transmission. Even though blockchain ensures transaction integrity, the actual data payload is encrypted before being exchanged between entities. This dual-layer security model protects both the integrity and privacy of shared information.

Another key feature of the proposed architecture is scalability. Intelligent systems often operate in large-scale environments involving thousands of devices and agents [8]. The framework supports distributed processing and parallel verification mechanisms, enabling efficient operation even in large networks with high transaction volumes.

IV. Experimental Setup

To evaluate the effectiveness of the proposed trust-aware blockchain framework, a simulated intelligent systems environment was developed. The experimental setup consisted of multiple intelligent agents representing distributed entities such as IoT devices, AI service providers, and data consumers. Each agent participated in secure data exchange transactions using the proposed framework.

The blockchain infrastructure was implemented using a private blockchain network consisting of several distributed nodes. Each node maintained a synchronized copy of the ledger and participated in consensus validation for new transactions. Smart contracts were deployed to enforce trust thresholds and manage access control policies during data exchanges.

The trust evaluation module was implemented using a weighted scoring model that considered factors such as historical reliability, transaction success rates, and anomaly detection results. Each participating entity was assigned a dynamic trust score that was updated after every interaction. Entities with trust scores below the defined threshold were restricted from participating in sensitive data exchanges.

To simulate real-world attack scenarios, malicious agents were introduced into the network. These agents attempted to inject falsified data or perform unauthorized transactions. The framework's ability to detect and isolate such entities was analyzed to measure its effectiveness in maintaining secure data exchange.

Performance metrics used in the evaluation included transaction latency, trust accuracy, attack detection rate, and data integrity preservation. The system was tested under varying network sizes and transaction loads to evaluate scalability and reliability.

The experimental environment was executed across distributed computing nodes to mimic real-world intelligent systems operating across different organizations and geographic locations.

V. Results and Discussion

The experimental results demonstrate that the proposed trust-aware blockchain framework significantly enhances the security and reliability of data exchange in intelligent systems. One of the key findings was the improvement in data integrity preservation [9]. Since all transactions were recorded on the blockchain, any attempt to modify stored information was immediately detected by the consensus mechanism.

The trust evaluation module successfully identified malicious agents within the network. Entities that attempted to submit falsified data experienced rapid trust score reductions, leading to automatic isolation through smart contract enforcement. This dynamic trust adaptation prevented compromised agents from repeatedly participating in malicious activities.

Another important observation was the transparency provided by the blockchain ledger. All participating entities could verify transaction histories and trust evaluations, increasing overall system accountability. This transparency reduced disputes among participants and improved collaborative decision-making.

In terms of performance, the framework demonstrated acceptable transaction latency even under increased network loads. While blockchain operations introduce additional computational overhead compared to centralized systems, the distributed architecture allowed parallel validation processes that minimized performance bottlenecks.

The attack detection rate observed in the experiments exceeded ninety percent for simulated malicious behaviors, indicating that the combination of trust analytics and blockchain verification is highly effective [10]. Compared with traditional centralized systems, the proposed architecture reduced unauthorized data exchange attempts by a substantial margin.

Overall, the results confirm that integrating blockchain with intelligent trust evaluation mechanisms provides a powerful solution for secure and reliable data exchange in distributed intelligent systems[11].

VI. Conclusion

The growing reliance on collaborative intelligent systems has created an urgent need for secure and trustworthy data exchange mechanisms. This research introduced a trust-aware framework that integrates blockchain technology with intelligent trust evaluation models to provide a secure and transparent environment for distributed data sharing. By combining immutable distributed ledgers with dynamic trust computation and automated smart contract enforcement, the proposed architecture ensures that only reliable entities participate in sensitive data exchanges while maintaining complete transaction transparency and data integrity. Experimental evaluation demonstrated that the framework effectively detects malicious participants, prevents unauthorized data manipulation, and maintains reliable system performance even under high network loads. The results highlight the potential of blockchain-enabled trust frameworks to support secure collaboration across intelligent ecosystems such as IoT networks, AI-driven platforms, and distributed enterprise systems, paving the way for more resilient and trustworthy intelligent infrastructures in future digital environments.

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] 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.

[3] 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.

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

[5] 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.

[6] P. Evangelatos *et al.*, "Named entity recognition in cyber threat intelligence using transformer-based models," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021: IEEE, pp. 348-353.

[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] T.-L. Do, M.-K. Tran, H. H. Nguyen, and M.-T. Tran, "Potential attacks of DeepFake on eKYC systems and remedy for eKYC with DeepFake detection using two-stream network of facial appearance and motion features," *SN Computer Science,* vol. 3, no. 6, p. 464, 2022.

[9] 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.

[10] 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.

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