Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1833–1841
DOI : 10.47974/JIOS-2275

Optimization of data integrity and security in distributed databases using blockchain technology

Pawan Arunkumar Upadhye [@]
Department of Electronics and Telecommunication Engineering
Symbiosis Institute of Technology (SIT)
Symbiosis International (Deemed University)
Lavale
Pune 412115
Maharashtra
India

Dipannita Mondal [†]
Department of Artificial Intelligence - Data Science and Machine Learning
Dr. D. Y. Patil College of Engineering and Innovation
Talegaon
Pune 410507
Maharashtra
India

Suma Sidramappa Hosamani [§]
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

V. Shanthi [‡]
Department of Computer Science
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India

[@] *E-mail:* pawan.arunkumar@gmail.com
[†] *E-mail:* ddmondal2684@gmail.com
[§] *E-mail:* suma.hosamani@vit.edu
[‡] *E-mail:* shanthiv@maher.ac.in

Vimal Bibhu *
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Abstract

Distributed databases are still very hard to keep safe because of the chance of hacking, unauthorized access, and data being different on different computers. Blockchain technology looks like a good idea because it uses immutability, digital proof, and consensus-driven verification to make sure that trust and resiliency are maintained. This article discusses about optimization methods, mathematical formulas, and game-theoretic models that are used in distributed environment for the efficient way performing data integrity and computing. By mixing blockchain with optimization tools, the study shows that attacks are less likely to succeed, risks are reduced, and data is securely stored.

Subject Classification: *68Q06, 11T71, 35Q89.*

Keywords: *Blockchain, Data integrity, Distributed databases, Security optimization, Game theory.*

1. Introduction

The rapid growth of distributed databases has changed how companies manage, store, and share data across many nodes that are all connected to each other [1]. These systems are good because they can grow, stay up for a long time, and work quickly, but they have a hard time keeping data safe. Since distributed databases aren't all in one place, they can be changed, accessed by people who shouldn't be able to, and have stability issues that make them less reliable [2, 3, 4]. Even though some traditional security measures, like encryption and access control, work, they often aren't enough to keep up with the changing threats of modern hacking [5, 6]. Its decentralised design works well with spread databases, making sure that data is available, safe, and can be fixed when something goes wrong [7, 8].

2. Optimization Approaches for Data Integrity and Security

Data Integrity and Security Optimization in distributed blockchain-enabled databases refers to designing a mathematical framework that minimizes security risks while maximizing integrity, availability, and performance through cryptographic and consensus mechanisms [9, 10]. Figure 1 shows the Multicolor Architecture.

* *E-mail:* **vimal.bhibu@niu.edu.in (Corresponding Author)**

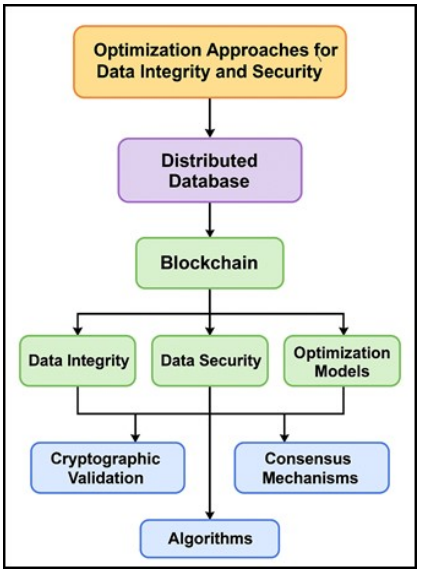

Figure 1

Multicolor Architecture of Optimization Approaches for Data Integrity and Security in Blockchain-Enabled Distributed Databases

Let database system be represented as:

$$D = \{d1, d2, \ldots, dn\}, di \in \mathbb{R}^m$$

Define security risk function:

$$R(D) = \Sigma\ (pi * vi)$$

where pi = probability of attack, vi = vulnerability weight

Define integrity function:

$$I(D) = \frac{(Valid\ Transactions)}{(Total\ Transactions)}$$

Confidentiality metric using entropy:

$$C(D) = -\Sigma\ P(xj) * \log\big(P(xj)\big) \quad (1)$$

Availability function:

$$A(D) = \frac{Uptime}{(Uptime + Downtime)} \quad (2)$$

Objective security utility function:

$$U = \alpha I(D) + \beta C(D) + \gamma A(D) - \lambda R(D) \quad (3)$$

where α, β, γ, λ are weighting factors

Optimization problem formulation:

Maximize U over D

Constraint – blockchain immutability condition:

$$T(i+1).hash = H(Ti\,|datai|) \tag{4}$$

Constraint – consensus validation:

$$\Sigma\, vk \geq \theta$$

where M = validators, θ = threshold

Lagrangian formulation:

$$L = U + \mu\left(T(i+1).hash - H(Ti\,|datai|)\right) + \nu\,(\Sigma\, vk - \theta) \tag{5}$$

KKT Conditions:

$$\nabla D\; L = 0, \mu \geq 0, \nu \geq 0$$

Optimal solution for secure integrity state:

D* = argmax U subject to immutability and consensus constraints

Theorem: *If blockchain consensus and immutability constraints hold, then the optimized utility function U guarantees maximized data integrity and minimized risk in distributed databases [11].*

Proof: From step (6),

$$U = \alpha I + \beta C + \gamma A - \lambda R \tag{6}$$

Since immutability ensures transaction validity,

$$I \rightarrow 1$$

Consensus ensures R(D) → 0 because adversaries cannot override majority validators.

Substituting in (6):

$$U* = \alpha(1) + \beta C + \gamma A - \lambda(0) \geq U \tag{7}$$

Therefore, the optimal utility U* is maximized under blockchain rules.

Hence, theorem holds.

3. Mathematical Formulation and Models

3.1. *Security Optimization Problem*

By reducing weaknesses, increasing robustness, and using blockchain's unchangeable record with cryptographic confirmation methods, the security optimization problem makes sure that the data in distributed systems is as accurate as possible [12, 13].

Let database system = D = {d1, d2, …, dn}

Define attack probability:

$$pi \in [0,1]$$

Define vulnerability weight:

$$vi \in \mathbb{R}+$$

Risk function:

$$R(D) = \Sigma\,(pi * vi) \tag{8}$$

Integrity function:

$$I(D) = \frac{Valid}{Total} \tag{9}$$

Confidentiality:

$$C(D) = -\Sigma P(xj)\log\big(P(xj)\big) \tag{10}$$

Availability:

$$A(D) = \frac{Uptime}{(Uptime + Downtime)} \tag{11}$$

Security utility function:

$$U = \alpha I(D) + \beta C(D) + \gamma A(D) - \lambda R(D) \tag{12}$$

Constraint – immutability:

$$T(i+1).hash = H(Ti\,|datai|) \tag{13}$$

Constraint – consensus:

$$\Sigma\, vk \geq \theta$$

Optimal secure state:

$$D* = argmax\, U$$

3.2. *Optimization Problem:*

The optimisation problem is to find the best balance between security, speed, and processing costs in blockchain-enabled systems while keeping data access, integrity, and strong defence against risks from bad actors.

Define objective function: f(D) = U

Variables: decision vector x ∈ ℝn

Constraints:

$$g(x) \leq 0, h(x) = 0$$

Risk minimization:

$$\min R(D) = \Sigma\ (pi\ *\ vi) \tag{14}$$

Integrity maximization:

$$\max I(D) = \frac{Valid}{Total} \tag{15}$$

Multi-objective formulation:

$$\max[I(D), C(D), A(D)]\ , \min R(D) \tag{16}$$

Scalarization:

$$F(D) = w1I(D) + w2C(D) + w3A(D) - w4R(D) \tag{17}$$

Feasible set:

$$X = \{x \mid g(x) \leq 0, h(x) = 0\} \tag{18}$$

Lagrangian:

$$L(x, \mu, v) = F(x) + \mu g(x) + vh(x) \tag{19}$$

First-order condition:

$$\nabla x\ L(x, \mu, v) = 0$$

KKT conditions:

$$\mu \geq 0, \mu g(x) = 0$$

Optimal solution:

$$x * \in X\ such\ that\ F(x *) \geq F(x), \forall\ x\ \in X$$

3.3. *Game-Theoretic Security Model*

The game-theoretic security model looks at how defenders and attackers plan to act strategically. It then optimises blockchain protocols to reach equilibrium, which protects data integrity, makes the system more resilient, and keeps it stable over time.

Define two players: Defender (D) and Attacker (A)

Strategy sets:

$$SD = \{sD1, sD2, \ldots\}, SA = \{sA1, sA2, \ldots\}$$

Payoff function Defender:

UD(sD, sA)

Payoff function Attacker:

UA(sD, sA)

Zero-sum assumption:

$$UD + UA = 0$$

Mixed strategy distribution:

$$PD, PA$$

Expected payoff Defender:

$$E[UD] = \Sigma\, PD(sD)\Sigma\, PA(sA)UD(sD, sA) \tag{20}$$

Nash equilibrium condition:

$$UD(sD*, sA*) \geq UD(sD, sA*), \forall\, sD$$

Equilibrium strategy:

$$(sD*, sA*) \in SD \times SA$$

4. Result Discussion

The results make it clear that blockchain-based methods work better than old-fashioned security and access control.

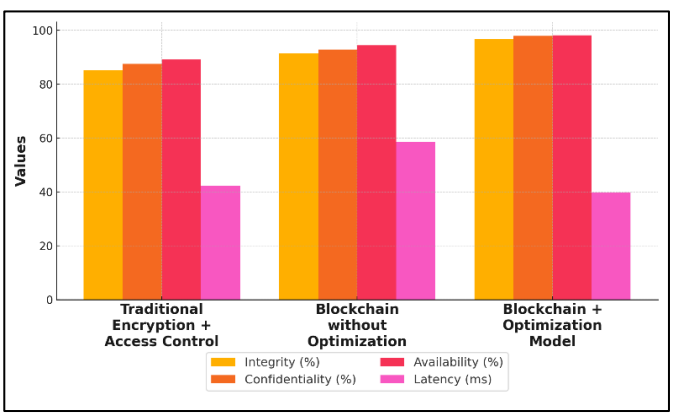

Figure 2
Comparison of Security Metrics and Latency Across Methods

Traditional methods offer average levels of integrity (85.2%), confidence (87.6%), and access (89.1%), but they still leave holes that can be exploited (in Figure 2).

If you don't optimise blockchain, it gets better, with higher security levels like 91.4% integrity and 94.5% availability, but at the cost of more delay (58.6 ms) (shows in Figure 3). The optimised blockchain model does much better than others. It has high integrity (96.7%), confidentiality (97.9%), and availability (98.2%), and it cuts delay (39.7 ms), which makes it both efficient and safe.

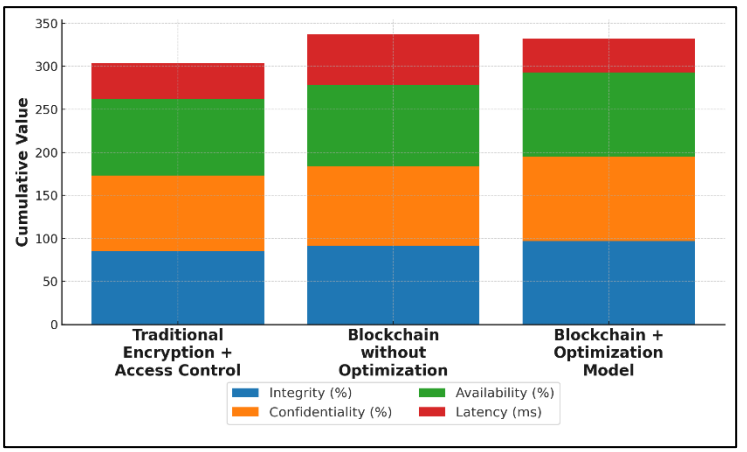

Figure 3
Cumulative Performance and Latency by Security Method

5. Conclusion

By using immutability, agreement, and cryptographic methods, this study shows how blockchain technology can improve the security and stability of data in distributed systems. The framework finds a balance between speed, security, and computing costs while reducing hostile risks. It does this by using optimisation techniques and game-theoretic models. The results show that blockchain can make computer systems that are reliable, open, and honest. Blockchain could become a key part of safe distributed data management with more work being done on scaling, mixed consensus protocols, and domain-specific apps in the future.

References

[1] A. G. Anagnostakis, N. Giannakeas, M. G. Tsipouras, E. Glavas, and A. T. Tzallas, "IoT micro-blockchain fundamentals," *Sensors*, vol. 21, p. 2784 (2021).

[2] T. Hristova, "Tracking mining company electric vehicles for sustainable development optimization using distributed ledger technologies," *J. Sustain. Min.*, vol. 23, pp. 299–314 (2024).

[3] S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, "Research and applied perspective to blockchain technology: A comprehensive survey," *Appl. Sci.*, vol. 11, p. 6252 (2021).

[4] X. Wang, W. Ni, X. Zha, G. Yu, R. P. Liu, N. Georgalas, and A. Reeves, "Capacity analysis of public blockchain," *Comput. Commun.*, vol. 177, pp. 112–124 (2021).

[5] A. S. Shete, S. Bhutada, M. B. Patil, P. H. Sen, N. Jain, and P. Khobragade, "Blockchain technology in pharmaceutical supply chain: Ensuring transparency, traceability, and security," *J. Stat. Manage. Syst.,* vol. 27, no. 2, pp. 417–428 (2024), doi: 10.47974/JSMS-1266.

[6] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, and Z. Ming, "Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach," *IEEE Internet Things J.*, vol. 8, pp. 2226–2237 (2020).

[7] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open J. Comput. Soc.,* vol. 3, pp. 122–136 (2022).

[8] S. Kumar, W. M. Lim, U. Sivarajah, and J. Kaur, "Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis," *Inf. Syst. Front.,* vol. 25, pp. 871–896 (2023).

[9] H. Xu, J. Wu, Q. Pan, X. Guan, and M. Guizani, "A survey on digital twin for industrial internet of things: Applications, technologies and tools," *IEEE Commun. Surv. Tutor.,* vol. 25, pp. 2569–2598 (2023).

[10] Z. A. Abdulrazzaq, M. S. Nayef, and M. Hbaib, "On semi-continuous and quasi-semi-continuous modules," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 4-A, pp. 1051–1058 (2025), doi: 10.47974/JDMSC-2031.

[11] S. Bhattacharya, L. Indise, N. Pandey, B. M. Nanche, S. Ramakrishna, and G. Sethi, "Analyzing the performance of wireless sensor networks using polynomial cryptography methods," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-A, pp. 563–570 (2026), doi: 10.47974/JDMSC-2497.

[12] A. Pasdar, Y. C. Lee, and Z. Dong, "Connect API with blockchain: A survey on blockchain oracle implementation," *ACM Comput. Surv.,* vol. 55, pp. 1–39 (2023).

[13] A. M. Pawar and N. Sherje, "Blockchain-based digital identity management systems," *Int. J. Adv. Comput. Eng. Commun. Technol.* (IJACECT), vol. 12, no. 2, pp. 1–7 (Apr. 2025).

Received April, 2025