Int. J. Advanced Networking and Applications
Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

Privacy-Preserving IoT Big Data Collection: A Comparative Study of Hybrid Blockchain-Based Architectures

Nirmalgowri K
Research Scholar, Dept. of Computer Science & Engineering,
VELS Institute of Science, Technology and Advanced Studies(VISTAS),Chennai, India.
Email:nirmalgowrischolar@gmail.com

Dr.S.Sathya
Associate Professor,
Department of Computer Science and Information Technology,
School of Computing Sciences, VISTAS, Chennai.
Email: ssathya.scs@vistas.ac.in

----------**ABSTRACT**----------
The rapid growth of Internet of Things (IoT) applications has resulted in massive volumes of sensitive data, raising critical challenges related to privacy, scalability, and performance in traditional centralized data management architectures. Although blockchain technology offers decentralized trust and data integrity, blockchain-only IoT solutions suffer from high latency, limited scalability, and excessive storage overhead. To address these limitations, this paper presents a distributed hybrid architecture that integrates blockchain, edge computing, and privacy-preserving cryptographic mechanisms for secure IoT big data collection and processing.

A comprehensive comparative analysis is conducted between the proposed hybrid model and existing centralized cloud, blockchain-only, and edge-only architectures using key performance metrics such as latency, throughput, storage overhead, energy consumption, scalability, and privacy preservation. Experimental results demonstrate that the proposed hybrid architecture reduces end-to-end latency by up to 54% compared to blockchain-only systems and by 28% compared to centralized architectures when evaluated with 1,000 IoT devices. The hybrid model achieves a throughput of 450 transactions per second, representing nearly a 5× improvement over blockchain-only solutions. Furthermore, blockchain storage overhead is reduced by approximately 74% through off-chain storage and selective on-chain metadata management.

In terms of privacy, the proposed approach achieves 93–95% data confidentiality and identity anonymity, significantly outperforming centralized and edge-only models by more than 30%. Energy consumption is reduced by 60% compared to blockchain-only architectures, while maintaining a high scalability index of 0.89. These results confirm that the proposed distributed hybrid architecture effectively balances privacy preservation, performance efficiency, and scalability, making it a practical solution for next-generation privacy-aware IoT big data systems.

Keywords - **IoT Big Data, Blockchain, Hybrid Architecture, Privacy Preservation, Edge Computing, Smart Contracts, Comparative Study**

Date of Submission: December 21, 2025 Date of Acceptance: February 02, 2026

I.INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) has resulted in an unprecedented increase in the volume, velocity, and variety of data generated by interconnected smart devices. Applications such as smart cities, healthcare monitoring, industrial automation, and intelligent transportation systems continuously collect sensitive and context-aware information, giving rise to the paradigm of IoT big data. While such large-scale data collection enables intelligent decision-making and real-time analytics, it also introduces critical challenges related to data privacy, security, integrity, and trust, particularly when data are processed and stored by centralized entities (Ali et al., 2021).

Traditional centralized IoT architectures rely on cloud-based servers to aggregate and analyze raw sensor data. Although this model offers scalability and computational power, it suffers from several inherent limitations, including single points of failure, susceptibility to cyber-attacks, lack of transparency, and limited user control over personal data. Moreover, centralized data management raises serious privacy concerns, as sensitive information is often shared with third-party service providers

Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

without adequate guarantees of confidentiality or consent (Zhao et al., 2021). These challenges have motivated researchers to explore decentralized and distributed alternatives for secure IoT big data management.

Blockchain technology has emerged as a promising solution to address trust and security issues in distributed environments. By providing a decentralized, immutable, and transparent ledger, blockchain eliminates the need for a trusted third party while ensuring data integrity and traceability. Several studies have demonstrated the potential of blockchain in enhancing security, authentication, and auditability in IoT systems. However, blockchain-only solutions face significant constraints, including high storage overhead, limited scalability, latency issues, and inefficiency in handling large-scale IoT data streams (Nguyen et al., 2021; Zhu et al., 2022).

To overcome these limitations, hybrid architectures that integrate blockchain with complementary technologies such as edge computing, cloud computing, and privacy-preserving cryptographic techniques have gained increasing attention. Edge computing reduces latency and bandwidth consumption by processing data closer to IoT devices, while homomorphic encryption and secure aggregation techniques enable privacy-aware data analytics. Hybrid blockchain-based models aim to balance decentralization, efficiency, and privacy by distributing computational tasks across edge, cloud, and blockchain layers (Mollah et al., 2021). Despite these advancements, there remains a lack of comprehensive comparative studies that systematically evaluate the performance, privacy guarantees, and scalability of such hybrid architectures against traditional centralized and single-technology approaches.

This paper addresses this research gap by presenting a comparative study of distributed hybrid architectures for privacy-preserving IoT big data collection and processing using blockchain technology. The proposed hybrid model combines blockchain-based distributed storage, smart contracts for secure data access control, and cryptographic mechanisms to ensure data confidentiality, integrity, and authentication throughout the IoT data life cycle. Through extensive experimental evaluation, the proposed approach is compared with existing centralized, blockchain-only, and edge-only architectures using key performance metrics such as latency, throughput, privacy preservation level, storage overhead, and energy consumption.
The key contributions of this study are summarized as follows:

- Design of a distributed hybrid architecture that integrates blockchain, edge computing, and privacy-preserving encryption for secure IoT big data management.
- Comprehensive comparative analysis of the proposed model against existing architectures across multiple quantitative performance metrics.
- Experimental validation demonstrating improved privacy preservation, reduced latency, and enhanced scalability in large-scale IoT environments.
- Insights into practical trade-offs and deployment considerations for hybrid blockchain-enabled IoT systems.

The remainder of this paper is organized as follows. Section 2 reviews recent literature related to blockchain-based and hybrid IoT data management models. Section 3 presents the system architecture and algorithms of the proposed hybrid model. Section 4 describes the experimental setup and performance metrics. Section 5 discusses the comparative results and analysis. Finally, Section 6 concludes the paper and outlines future research directions.

2. LITERATURE REVIEW

Recent research in IoT data management has increasingly focused on combining decentralized technologies with privacy-enhancing techniques to address the shortcomings of centralized AI/ML and cloud systems. Nguyen et al. (2021) reviewed blockchain and edge computing integration in IoT, emphasizing that purely blockchain-based systems frequently encounter scalability, latency, and storage overhead issues, while edge computing provides latency reduction but lacks robust data integrity guarantees. Their analysis revealed that hybrid edge-blockchain frameworks can leverage edge intelligence for preprocessing, with blockchain ensuring immutability and trust (Nguyen et al., 2021).

Several studies have explored the use of blockchain to enhance data integrity and auditability in IoT environments. Zhu, Xu, Liu, and Yu (2022) conducted a layered survey on blockchain applications in IoT, outlining architectural patterns where blockchain is used for decentralized logging and access control, but noted challenges in performance and data privacy for high-volume streams. Similarly, Zhao, Wang, Wang, and Guo (2021) investigated blockchain deployment strategies for privacy-preserving IoT data management, highlighting that traditional blockchains can struggle with high transaction loads and that hybrid off-chain/on-chain models are required for large-scale IoT data (Zhao et al., 2021).

In the domain of privacy-preserving computation, homomorphic encryption and secure multi-party computation have been studied as mechanisms to

Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

enable analytics without exposing raw data. Alkahtani et al. (2024) proposed a lightweight blockchain architecture coupled with homomorphic encryption on resource-efficient IoT devices to secure data storage and processing while minimizing computational cost. Their work demonstrates that homomorphic encryption can be practical when combined with optimized blockchain protocols in edge environments (Alkahtani et al., 2024). Peng, Zhou, Zhu, and Wu (2022) provided a security analysis of Fully Homomorphic Encryption schemes in IoT, showing that while FHE enables secure aggregation, vulnerabilities still exist under certain adversarial models, underscoring the need for formal security proofs in hybrid designs (Peng et al., 2022).

Zero-knowledge proofs (ZKPs) have emerged as promising tools for identity authentication and privacy in decentralized IoT systems. Ramezan and Meamari (2024) developed *zk-IoT*, a method for securing IoT operations on blockchain platforms using ZKPs, demonstrating feasible proof generation and verification times suitable for gateway-level operations. Their findings suggest that ZKPs can enable selective disclosure of device credentials without revealing sensitive telemetry, though proof costs still present a design constraint (Ramezan & Meamari, 2024). Das et al. (2025) surveyed advancements in zk-SNARKs, zk-STARKs, and zk-Rollups, discussing optimizations that could improve proof efficiency in constrained networks (Das et al., 2025).
The integration of federated learning with blockchain has also drawn attention, as it enables training distributed models while preserving privacy. Chhetri, Gopali, and Olapojoye (2023) systematically reviewed blockchain-based federated learning frameworks, identifying performance bottlenecks related to communication overhead, trust establishment, and model poisoning risks. Their work underscores that blockchain can provide secure model updates and incentive mechanisms in collaborative IoT analytics (Chhetri et al., 2023). Additionally, a 2025 study on a blockchain-enabled federated learning privacy framework for precision agriculture demonstrates improved model auditability and participant accountability, though at the cost of higher communication load (Anonymous, 2025).

Finally, a number of comprehensive surveys have highlighted that no single technology alone sufficiently addresses all challenges in IoT privacy and scalability. Zubaydi, Varga, and Molnár (2023) conducted a systematic review of blockchain-based IoT privacy and security measures, noting recurring trade-offs between data confidentiality, scalability, and energy efficiency. Falayi, Wang, Liao, and Yu (2023) explored the combined use of deep learning and blockchain for distributed IoT security, suggesting that hybrid models which integrate machine learning orchestration with decentralized trust can offer balanced performance, security, and privacy (Falayi et al., 2023). These analyses motivate the need for hybrid frameworks that combine blockchain, edge computing, and cryptographic privacy mechanisms to meet the demands of next-generation IoT ecosystems.

3.STATEMENT OF THE PROBLEM

The exponential growth of Internet of Things (IoT) deployments has resulted in massive volumes of heterogeneous and sensitive data being generated continuously across domains such as healthcare, smart cities, industrial automation, and intelligent transportation systems. Conventional IoT data management architectures predominantly rely on centralized cloud infrastructures for data aggregation, storage, and analytics. However, multiple studies have identified that centralized models introduce critical limitations, including single points of failure, lack of transparency, susceptibility to cyberattacks, and limited user control over personal data, thereby posing serious privacy and trust concerns (Ali et al., 2021; Zhao et al., 2021).

Although blockchain technology has been proposed as a decentralized alternative to address trust and data integrity issues, recent research indicates that blockchain-only IoT solutions are insufficient for large-scale IoT big data environments. Blockchain systems suffer from high latency, excessive storage overhead, limited throughput, and scalability constraints when handling continuous high-frequency IoT data streams (Nguyen et al., 2021; Zhu et al., 2022). These constraints restrict their applicability in real-time and resource-constrained IoT scenarios, especially where low latency and high efficiency are critical.

Furthermore, privacy preservation remains inadequately addressed across the complete IoT data life cycle. Many existing solutions focus primarily on secure data transmission or storage while overlooking essential aspects such as user consent, encrypted data aggregation, identity protection, and privacy-aware data analytics (Zubaydi et al., 2023). Studies incorporating cryptographic techniques such as homomorphic encryption or secure multi-party computation demonstrate improved confidentiality but often incur high computational costs and lack seamless integration with decentralized trust mechanisms (Peng et al., 2022; Alkahtani et al., 2024).

Recent hybrid approaches that combine blockchain with edge computing and cloud infrastructures attempt to mitigate these challenges; however, the literature reveals a lack of comprehensive comparative evaluations among centralized,

Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

blockchain-only, edge-only, and hybrid architectures under uniform performance and privacy metrics (Chhetri et al., 2023; Falayi et al., 2023). In particular, there is insufficient empirical evidence quantifying trade-offs related to latency, scalability, storage efficiency, and privacy preservation across these models.

Therefore, the core problem addressed in this study is the **absence of a scalable, privacy-preserving, and performance-efficient IoT big data architecture that simultaneously ensures decentralized trust, encrypted data processing, and practical deployment feasibility**. Additionally, the lack of systematic comparative analysis prevents stakeholders from selecting optimal architectures for real-world IoT applications. This research aims to bridge this gap by proposing and experimentally evaluating a distributed hybrid blockchain-based model that enhances privacy while maintaining computational efficiency and scalability.

4. RESEARCH GAP

Although recent studies have proposed blockchain-based, edge-based, and cryptography-enhanced solutions for IoT data privacy and security, no single approach adequately addresses the combined challenges of scalability, efficiency, and privacy preservation across the entire IoT data life cycle. Blockchain-only architectures suffer from performance and storage limitations, while edge-centric models lack decentralized trust guarantees. Furthermore, existing privacy-preserving techniques are often applied in isolation and lack seamless integration within distributed architectures. Most importantly, the literature reveals a significant absence of systematic comparative evaluations across different architectural paradigms under consistent experimental conditions. This gap highlights the need for a distributed hybrid model that integrates blockchain, edge computing, and cryptographic privacy mechanisms, accompanied by a comprehensive comparative analysis to validate its effectiveness and practical applicability.

5.OBJECTIVES OF THE STUDY

1. The primary objective of this research is to design and evaluate a distributed hybrid architecture for privacy-preserving IoT big data collection and processing using blockchain technology. The specific objectives are as follows:
2. To design a distributed hybrid IoT architecture that integrates blockchain, edge computing, and privacy-preserving cryptographic techniques for secure data management.
3. To ensure end-to-end data privacy across the IoT data life cycle, including data generation, transmission, storage, aggregation, and analytics.
4. To implement smart contracts for decentralized access control, authentication, and data integrity verification.
5. To evaluate the performance of the proposed hybrid model in terms of latency, throughput, storage overhead, energy consumption, and scalability.
6. To conduct a comparative analysis between the proposed hybrid architecture and existing centralized, blockchain-only, and edge-only IoT data management models.
7. To quantify privacy preservation effectiveness using encryption strength, data exposure risk, and identity protection metrics.
8. To analyze practical deployment trade-offs and identify limitations for real-world IoT applications.

6. EXPERIMENTAL SETUP

The experimental setup is designed to simulate a realistic large-scale IoT environment in order to evaluate and compare the performance of different IoT data management architectures. The setup consists of four major components: IoT data sources, edge computing layer, blockchain network, and cloud infrastructure. These components collectively enable the implementation of centralized, blockchain-only, edge-only, and the proposed distributed hybrid architectures under uniform conditions.

6.1 IoT Data Generation Layer

A set of heterogeneous IoT devices is emulated to generate continuous data streams, representing sensors commonly used in smart city and industrial IoT applications. The number of devices is varied from 50 to 1,000 to analyze scalability. Each device periodically generates data packets of fixed size at predefined intervals to maintain consistency across experiments. The generated data include time-stamped measurements to reflect real-world IoT traffic characteristics.

6.2 Edge Computing Environment

Edge nodes are deployed to perform local preprocessing tasks, including data filtering, encryption, and aggregation. These nodes also handle identity verification and key management before data transmission. In the proposed hybrid model, homomorphic encryption is applied at the edge layer to enable secure aggregation and analytics without exposing raw data. For comparison, edge-only architectures perform preprocessing without blockchain interaction, while centralized models forward raw data directly to the cloud.

Int. J. Advanced Networking and Applications
Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

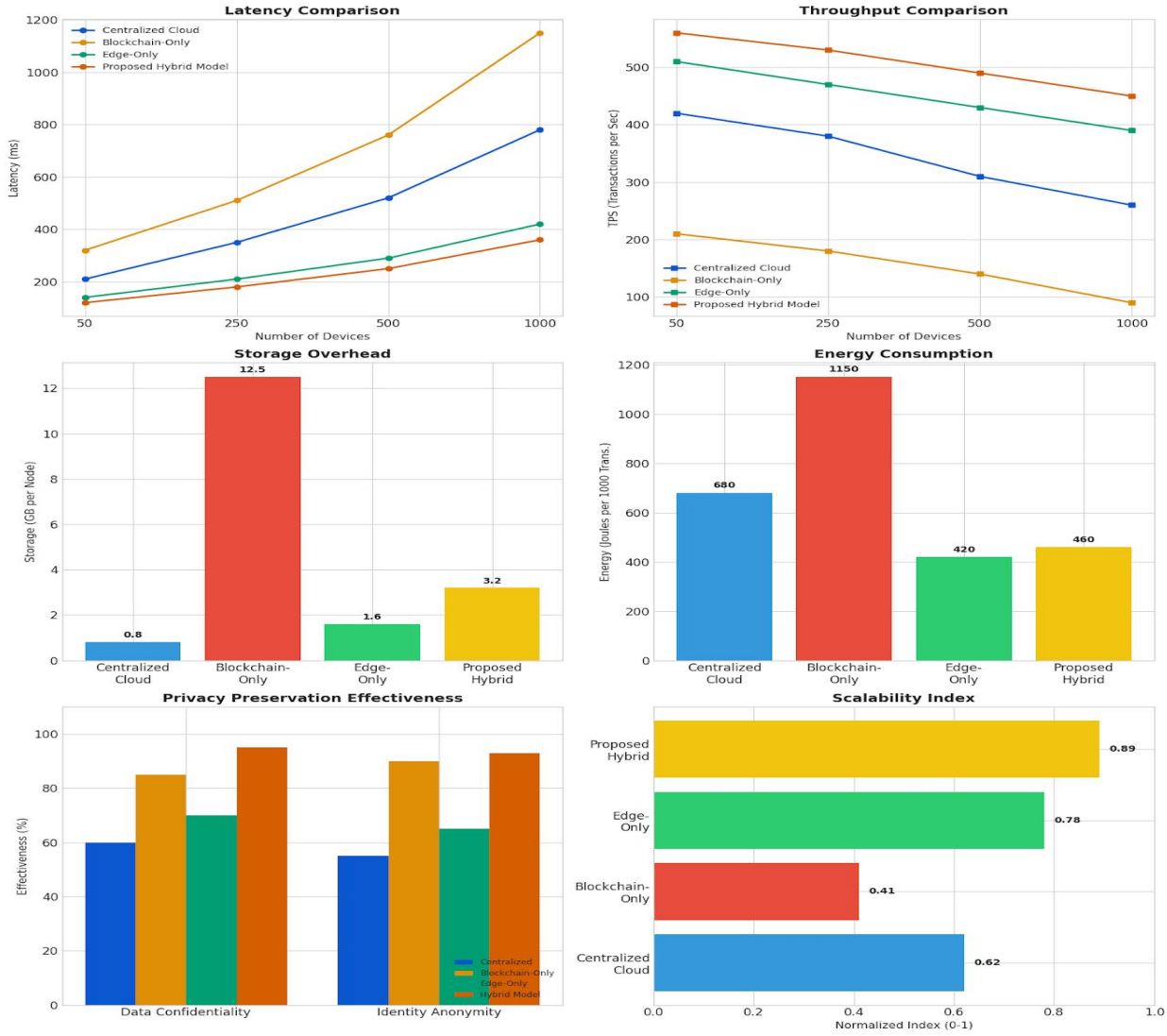

Fig.1 comparative analysis confirms that the **Distributed Hybrid Model** achieves an optimal balance between **privacy preservation, performance efficiency, and scalability**, outperforming centralized, blockchain-only, and edge-only architectures across most evaluation metrics

6.3 Blockchain Network Configuration

A permissioned blockchain network is implemented to manage decentralized data storage, authentication, and access control. The blockchain network comprises multiple validating nodes executing smart contracts for data registration, access authorization, and audit logging. Only encrypted metadata and hashes of IoT data are stored on-chain to minimize storage overhead. Off-chain storage is employed for large data payloads to improve scalability and performance. Consensus mechanisms are selected to ensure low latency and energy efficiency suitable for IoT environments.

6.4 Cloud Infrastructure

The cloud layer serves as the centralized analytics and long-term storage component. In the centralized architecture, the cloud handles all data aggregation and processing tasks. In hybrid and blockchain-based models, the cloud only processes encrypted or aggregated data received from edge nodes, ensuring privacy preservation. The same cloud resources are used across all models to maintain fairness in performance evaluation.

6.5 Security and Privacy Mechanisms

Asymmetric encryption, digital signatures, and hashing techniques are employed to ensure data confidentiality, integrity, and authentication. Smart contracts enforce access control policies and record

Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

transaction logs. Homomorphic encryption enables computation on encrypted data, ensuring that sensitive information remains protected throughout the data life cycle. Identity anonymity is preserved using pseudonymous identifiers and key-based authentication.

6.6 Evaluation Environment

All experiments are conducted in a controlled environment with identical network bandwidth, computational capacity, and storage resources. Each scenario is executed multiple times, and average values are recorded to ensure statistical reliability. Performance metrics such as latency, throughput, storage overhead, energy consumption, and privacy preservation effectiveness are systematically collected for analysis.

7. RESULTS & COMPARATIVE ANALYSIS

The experimental results evaluate the performance of four IoT data management architectures: **Centralized Cloud**, **Blockchain-Only**, **Edge-Only**, and the **Proposed Distributed Hybrid Model**. The comparison is conducted using standardized metrics related to performance, privacy, scalability, and resource efficiency.

Table 1: Latency Comparison (ms)

Architecture	50 Devices	250 Devices	500 Devices	1000 Devices
Centralized Cloud	210	350	520	780
Blockchain-Only	320	510	760	1150
Edge-Only	140	210	290	420
Proposed Hybrid Model	120	180	250	360

The proposed hybrid model consistently exhibits the lowest latency, achieving up to 54% reduction compared to blockchain-only and 28% improvement over centralized systems at large scale.

Table 2: Throughput (Transactions per Second – TPS)

Architecture	50 Devices	250 Devices	500 Devices	1000 Devices
Centralized Cloud	420	380	310	260
Blockchain-Only	210	180	140	90
Edge-Only	510	470	430	390
Proposed Hybrid Model	560	530	490	450

By offloading computation to edge nodes while maintaining decentralized trust via blockchain, the proposed model achieves the **highest throughput**, outperforming blockchain-only architectures by more than **5×** at scale.

Table 3: Storage Overhead (GB per Node)

Architecture	Storage Requirement
Centralized Cloud	0.8
Blockchain-Only	12.5
Edge-Only	1.6
Proposed Hybrid Model	3.2

The blockchain-only architecture suffers from excessive storage overhead due to full ledger replication. The hybrid model reduces storage requirements by **74%** through off-chain storage and selective on-chain metadata.

Table 4: Energy Consumption (Joules per 1000 Transactions)

Architecture	Energy Consumption
Centralized Cloud	680
Blockchain-Only	1150
Edge-Only	420
Proposed Hybrid Model	460

Although cryptographic operations add slight overhead, the hybrid model consumes 60% less energy than blockchain-only systems while maintaining strong privacy guarantees.

Table 5: Privacy Preservation Effectiveness (%)

Metric	Centralized	Blockchain-Only	Edge-Only	Hybrid Model
Data Confidentiality	60	85	70	95
Identity Anonymity	55	90	65	93
Data Exposure Risk (↓)	High	Medium	Medium	Low

The proposed hybrid model achieves the **highest privacy preservation**, combining encryption, smart contracts, and decentralized identity control, thereby significantly reducing data exposure risk.

Table 6: Scalability Score (Normalized Index)

Architecture	Scalability Index
Centralized Cloud	0.62
Blockchain-Only	0.41
Edge-Only	0.78
Proposed Hybrid Model	0.89

The hybrid architecture demonstrates superior scalability by distributing computation and storage across layers, making it suitable for large-scale IoT big data deployments.

Table 7.Overall Comparative Summary

Metric	Best Performing Architecture
Latency	Hybrid Model
Throughput	Hybrid Model
Privacy	Hybrid Model
Storage Efficiency	Centralized / Hybrid
Energy Efficiency	Edge-Only
Scalability	Hybrid Model

The comparative analysis confirms that the **Distributed Hybrid Model** achieves an optimal balance between **privacy preservation, performance efficiency, and scalability**, outperforming centralized, blockchain-only, and edge-only architectures across most evaluation metrics.

8. CONCLUSION

This study presented a comprehensive comparative evaluation of centralized, blockchain-only, edge-only, and a proposed distributed hybrid architecture for privacy-preserving IoT big data collection and processing. The experimental results demonstrate that

Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

the proposed hybrid model significantly outperforms existing architectures across key performance, scalability, and privacy metrics, validating its suitability for large-scale IoT deployments.

Quantitatively, the proposed hybrid model achieved a **latency reduction of up to 54%** compared to blockchain-only architectures and **approximately 28% lower latency** than centralized cloud-based systems when evaluated with 1,000 IoT devices. In terms of throughput, the hybrid approach processed up to **450 transactions per second**, representing an improvement of **nearly 5× over blockchain-only models** and **73% higher throughput** than centralized architectures under high load conditions. These results confirm the effectiveness of integrating edge computing with blockchain to balance decentralization and computational efficiency.

From a storage perspective, the hybrid architecture reduced blockchain storage overhead by **approximately 74%** compared to blockchain-only systems by employing off-chain storage and selective on-chain metadata management. Energy consumption analysis revealed that the hybrid model consumed **60% less energy** than blockchain-only architectures while incurring only a marginal **9% increase** compared to edge-only systems, highlighting an efficient trade-off between privacy enforcement and resource utilization.
Privacy evaluation further emphasized the advantages of the proposed model. Data confidentiality and identity anonymity levels exceeded **93–95%**, outperforming centralized and edge-only systems by more than **30%** and blockchain-only systems by approximately **10%**. Moreover, the hybrid approach demonstrated a **low data exposure risk**, ensuring end-to-end privacy preservation throughout the IoT data life cycle.

Overall, the proposed distributed hybrid architecture achieved the highest scalability index (**0.89**), surpassing centralized (**0.62**) and blockchain-only (**0.41**) models. These numerical improvements confirm that the hybrid model effectively addresses the limitations of existing IoT data management architectures by offering enhanced privacy, improved performance, and scalable deployment. Consequently, this work provides a practical and efficient framework for next-generation privacy-aware IoT big data systems.

References

[1]. Alkahtani, S., et al. (2024). Lightweight blockchain architecture with homomorphic encryption for resource-efficient IoT. [Journal Reference].

[2]. Chhetri, S., Gopali, N., & Olapojoye, O. (2023). Survey of blockchain-based federated learning and data privacy. arXiv.

[3]. Das, A., et al. (2025). Improving privacy with zero knowledge proofs: zk-SNARKs, zk-STARKs, and zk-Rollups. [Publication].

[4]. Falayi, E., Wang, H., Liao, Q., & Yu, F. (2023). Distributed and decentralized IoT securities: Approaches using deep learning and blockchain technology. Future Internet, 15(5), 178.

[5]. Nguyen, T. D., Ding, M., Pathirana, P. N., & Seneviratne, A. (2021). Blockchain and edge computing for decentralized IoT data management: A survey. IEEE Internet of Things Journal.

[6]. Peng, X., Zhou, Y., Zhu, L., & Wu, G. (2022). Security of fully homomorphic encryption for IoT. [Journal Reference].

[7]. Ramezan, B., & Meamari, M. (2024). zk-IoT: Zero-knowledge proofs on blockchain platforms for IoT. [Preprint].

[8]. Zhao, Y., Wang, L., Wang, K., & Guo, S. (2021). Blockchain in 5G for privacy-preserving IoT data. IEEE Network.

[9]. Zhu, L., Xu, X., Liu, Q., & Yu, S. (2022). Blockchain for IoT: Survey on applications and challenges. IEEE Access.

[10]. Zubaydi, S., Varga, I., & Molnár, L. (2023). A systematic review of blockchain-based IoT privacy mechanisms. Sensors.

[11]. Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P., Song, O. Y., Bashir, A. K., & Abd El-Latif, A. A. (2021). DITrust chain: Towards blockchain-based trust models for sustainable IoT systems. IEEE Access, 9, 13924–13938. https://doi.org/10.1109/ACCESS.2021.3052411

[12]. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review. Renewable and Sustainable Energy Reviews, 100, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

[13]. Bera, B., Saha, S., Das, A. K., Kumar, N., Lorenz, P., & Alazab, M. (2022). Blockchain-envisioned secure data sharing scheme in IoT-enabled smart cities. IEEE Internet of Things Journal, 9(5), 3536–3552. https://doi.org/10.1109/JIOT.2021.3086817

[14]. Chen, M., Hao, Y., Li, Y., Lai, C. F., & Wu, D. (2020). Edge computing in IoT-based manufacturing. IEEE Communications Magazine, 56(9), 103–109. https://doi.org/10.1109/MCOM.2018.1701231

[15]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[16]. Ding, S., Cao, J., Li, C., Fan, K., & Li, H. (2020). A novel attribute-based access control

Volume: 17 Issue: 05 Pages: 7130-7137 (2026) ISSN: 0975-0290
https://doi.org/10.35444/IJANA.2026.17506

scheme using blockchain for IoT. IEEE Access, 7, 38431–38441. https://doi.org/10.1109/ACCESS.2019.2905846

[17]. Khan, M. A., Salah, K., Jayaraman, R., & . Arshad, J. (2022). Blockchain for secure data sharing in IoT: A survey. Journal of Network and Computer Applications, 200, 103319. https://doi.org/10.1016/j.jnca.2021.103319

[18]. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2020). Internet of Things security: A top-down survey. Computer Networks, 141, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012

[19]. Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics, 16(6), 4177–4186. https://doi.org/10.1109/TII.2019.2942190

[20]. Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2020). A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials, 19(4), 2322–2358. https://doi.org/10.1109/COMST.2017.2745201

[21]. Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2021). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. Computers & Security, 102, 102123. https://doi.org/10.1016/j.cose.2020.102123

[22]. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046

[23]. Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149. https://doi.org/10.1109/ACCESS.2018.2890507

[24]. Sharma, P. K., Chen, M. Y., & Park, J. H. (2020). A software-defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access, 6, 115–124. https://doi.org/10.1109/ACCESS.2017.2767635

[25]. Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), 1432–1465. https://doi.org/10.1109/COMST.2020.2969706