Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 3, 2026

HYBRID BLOCKCHAIN ARCHITECTURE FOR SECURE AND SCALABLE IOT DATA MANAGEMENT

Muhammad Saleh Shah*[1], Shafiq-Ur-Rehman Massan[2], Shahid Khan[3]

*[1]*Principle, Government College of Technology Larkano*
[2]*Chairman CSIS, Khadim Ali Shah Bukhari Institute of Technology, Karachi, Sindh*
[3]*Assistant Professor, Khadim Ali Shah Bukhari Institute of Technology, Karachi, Sindh*

*[1]salehshah@gmail.com, [2]srmassan@hotmail.com, [3]shahid@kasbit.edu.pk

DOI: https://doi.org/10.5281/zenodo.19044054

Keywords
Internet of Things (IoT); Hybrid Blockchain; Data Management; Security; Scalability.

Article History
Received: 05 January 2026
Accepted: 18 February 2026
Published: 16 March 2026

Copyright @Author
Corresponding Author: *
Muhammad Saleh Shah

Abstract

Massive emergence of Internet of Things (IoT) environments has aggravated the problems in terms of safe and scaled and efficient data administration. To address the weaknesses posed by the traditional centralized blockchain and single layer systems, the paper will show a hybrid blockchain architecture that integrates the public and private blockchain layer. The prototype of sensitive data management was implemented on the permissioned blockchain and the prototype of integrity validation on the public blockchain. It is experimentally evaluated because the suggested architecture improves the data processing speed by 40 percent, reduces the storage costs by 30 percent, and the authenticity of data by 99.9 percent. The analysis of security demonstrates that the 95 percent successful cyber-attack is mitigated in connection with the centralized IoT systems. The fact that scalability testing with higher density of devices demonstrated that this system can only increase its latency by 12 percent as the number of connected devices increase 50,000-fold, however, the sheer existence of the system demonstrates its soundness. To obtain the holistic analysis, Hybrid Blockchain Effectiveness Index (HBEI) was developed that comprised of four dimensions of security (0.40), scalability (0.30), data management (0.20), and interoperability (0.10) with the overall effectiveness score being 0.91. An economic analysis reveals that the investment is 4 times paid, which shows the economic sustainability of the utilization of hybrid blockchain. The findings confirm that hybrid blockchain infrastructure offers a moderate solution regarding decentralization, performance effectiveness, and enhanced security. The investigation offers a numerical data that can be referenced to the introduction of the hybrid blockchain integration as an effective and cost-effective approach in the future to manage the IoT data infrastructure in smart cities, healthcare, and IoT applications in the industries.

INTRODUCTION

This rapid development of Internet of Things (IoT) has resulted in a gradual flood of heterogeneous data of proportions vast in magnitude and smart equipment, sensors, and cyber-physical systems. It is estimated that currently, the number of IoT ecosystems is more than 70 percent of the real-time data transfer in the distributed computing setting and these create immense challenges in terms of secure storage, scalable processing, and dependable data transfer. The conventional centralized data management framework is gradually becoming incapable of meeting such requirements due to the growing prevalence of single points of failures, low-scale, and higher chances of cyber attack. As a result, the use of centralized data processing systems is found to have led to more than 55 percent of the reported IoT security breach cases (Sharma and Park, 2018).

Decentralization, immutability, and cryptographic verification can make the blockchain technology a solution to the data integrity and trust issue in the IoT environment. However, there are severe limitations to single blockchain applications. Public blockchains are low throughput, expensive and highly latent, but private blockchains are not very fast but have undermined the decentralization and transparency requirements. In a bid to overcome these shortcomings, hybrid blockchain architectures have experienced some interest as a result of their performance-security trade-offs. Since Nandanwar and Katarya (2025) demonstrate by more than 35 percent, hybrid blockchain structures increase the precision of intrusion detection in IoT systems, that is why they are useful in the environment with a high level of security concern.

A limited number of studies have examined hybrid blockchain solutions in healthcare and smart systems. Rathee et al. (2020) argue that the hybrid blockchain integration offers high efficiency in the multimedia data processing of the IoT-healthcare applications with the maximum latency reduction of 30 percent. Similarly, Jayabalan and Jeyanthi (2022) present an off-chain IPFS-compatible scalable blockchain design that reduces storage overhead by nearly 40 per cent, one of the inherent scalability bottlenecks of traditional blockchain designs. The importance of hybrid storage architecture is also mentioned in Zhou et al. (2022), which proves that semantic blockchain databases will enhance query time by 45 percent when the off-chain storage is scaled.

In addition to the efficiency in storage and processing, authentication and the access control are also relevant concerns in the data management of IoT. The article by Khan et al. (2025) offers a lightweight hybrid authentication system based on blockchain and edge computing that can achieve an authentication rate of more than 90 percent and low computing capabilities. Likewise, agrawal et al. (2024) also indicate that blockchain paired with fog computing and hybrid encryption also significantly help in providing control access to secure data in a distributed environment. These findings just indicate the need to have multi-layered hybrid architectures that may accommodate security, scalability and interoperability simultaneously.

The existence of these developments has, however, been the primary contributor to a discourse of area-specific applications, and has not given much consideration to the general performance analysis and also financial viability. Moreover, the possibility of interaction between hybrid blockchain systems and some of the largest data management platforms built on the IoT such as data lakes and hybrid clouds is not studied (Nuthalapati, 2023; Dhruvitkumar, 2021). The paper addresses the gaps by proposing a hybrid blockchain architecture to combine the public and the private blockchain to realize a secure and scalable system of managing IoT data as well as numerical blockchain performance analysis and cost-benefit analysis.

Research Questions

Why does a hybrid blockchain architecture in the IoT data management system have an advantage over security and scalability?

What is the degree of performance that can be achieved compared to a single-blockchain architecture?

Research Objectives

To establish and implement a hybrid blockchain system to integrate a public and a private blockchain to handle IoT data.

In order to quantify the performance on the system using quantitative metrics that are processing speed, storage efficiency, security and returns on investment (ROI).

Literature Review

The article by Golder et al. (2024) proposes a Hybrid Blockchain Framework of Secure and Scalable IoT Networks (HB-IoT) as a mix between a publicly and privately run blockchain layer to provide the solution to the issue of scalability and trust to the IoT ecosystem. They state that the transaction throughput improves by 38% and the validation latency reduce by 42% with the standalone models of the public blockchain. The framework can be used to depict a high degree of information confidentiality and resiliency by isolating sensitive IoT data to permissioned ledgers and upholding integrity evidence on the open chains. The authors however note that overheads of cross-chain coordination are approximately 12 times greater relative to large-scale deployment that interoperability mechanisms ought to be optimized in large-scale deployments.

The article by Sharmin and others (2025) is focused on highly sensitive to privacy and scalable hybrid blockchain in healthcare data management with regulatory compliance concerns and patient data privacy issues. The design of their design also makes them 99.8 percent accurate in the integrity of their data and 35 percent fewer redundancy of their storage off-chain encrypted repositories. The article finds out that operational expenses are reduced by 2530 percent when there is use of hybrid blockchain in comparison to the centralized healthcare information systems. It is an effective framework, but it is domain-specific and in the heterogeneous and heterogeneous IoT systems, where the latency and throughput requirements are different, it cannot be implemented directly.

Ali et al. (2023) extend the research of hybrid blockchain and integrate deep learning models into the study to broaden the scalability and anomaly detection of the blockchain-driven healthcare systems. The results as presented by them indicate that there is an accuracy of 45 percent and a reduction of 28 percent in the system response time as well as accuracy in detecting the attack when implemented compared to the conventional blockchain-based healthcare platforms. The hybrid model suggests that the blockchain and smart analytics may be used to increase the strength of the system to a significant extent. The higher computational load at 18 percent and the cost is an issue of concern when considering the energy efficiency of resource-constrained IoT networks. Several metaheuristic algorithms have been developed to solve complex optimization problems in engineering systems (Massan et al., 2020).

Haque et al. (2024) provide an IoT data management scheme based on scalable blockchain-based system on a lightweight consensus mechanism. Their technology reduces the execution time of consensus by 40 percent and energy consumption by 33 percent, which is suitable in large-scale IoT implementation. The article confirms that the hybrid consensus models possess a higher throughput and sustainability value compared to the traditional Proof-of-Work systems. The framework however is performance centered rather than interoperability centered and not much care is taken on the cross platform data exchange.

The article by Irshad et al. (2023) introduces an IoT-friendly secure and scalable cloud architecture that includes blockchain technology and post-quantum cryptography. Their hybrid character augments the system resilience of quantum-based attacks reducing 95 percent the cryptographic shortcomings. Multi-user access is also 30 percent more efficient with decentralized schemes of authentication in the suggested architecture. The security benefits are immense, but the authors acknowledge augmented complexity of systems and deployments costs that may impact the introduction of the emerging cost-sensitive market.

Taloba et al. (2023) propose an IoT-healthcare environment that presents the hybrid multimedia data processing platform that relies on blockchains. Their architecture is capable of supporting high volume multimedia streams with the lowest delay of the transmission of data of 37 and more efficient processing of 41. The hybrid architecture attains a good parameter of centralized processing of heavy workloads as compared to decentralized validation in security. Scalability testing was however tested on a medium-scale networks only which meant that there was a need to test it in ultra-large ecosystems of IoT.

Another hybrid architecture is also applied by Lee et al. (2024) to speak about storage limits related to the IoT in which decentralized data storage is combined with centralized management stages. As per their findings, storage overheads are reduced by half and desirable rate of data retrieval is enhanced by 45 percent. The hybrid approach will make it possible to effectively index metadata without sacrificing the benefits of decentralization. Despite the existence of such benefits, the centralized management aspect can become the only weak point, which must partially overcome the concept of decentralization of blockchain.

The hybrid centralized/blockchain-based authentication architecture of heterogeneous IoT networks developed by Khashan and Khafajah (2023) is effective. The success rates in authentication are 92 percent in their model and 34 percent less time is spent in verifying an access than in a fully decentralized authentication system. The article demonstrates that hybrid authentication structures are feasible in offering a performance and security compromise. Nevertheless, the framework does not exhaust the idea of scalability when scalability might happen in situations that involve extreme device density, and there is a gap in the research under hybrid blockchain-enabled IoT.

Research Methodology

Research Philosophy

The philosophy of the research is positivist since the work will be preoccupied with objective measurement, empirical analysis, and quantitative performance measurement of a hybrid blockchain architecture of managing the IoT data. Positivism would be appropriate as the parameters of the system performance (speed of processing, storage efficiency, accuracy of security and scalability) could be objectively measured and statistically analyzed. The philosophy is friendly to hypothesizing and measurement of architectural effectiveness.

Research Approach

The kind of research used is a deductive research in which the available theories regarding blockchain scalability, IoT security, and hybrid structures are adopted to arrive at a conceptual framework. According to this framework, performance hypothesis testing is conducted with the help of experimental implementation and numerical analysis. This approach will allow confirming the methodology about the possible improvement of the effect of data management of IoT by the integration of hybrid blockchain into the traditional architectures.

Research Strategy

It can be considered as an experimental and design-based study because it presupposes the development of a hybrid blockchain prototype that will be based on Hyperledger Fabric (private blockchain) and Ethereum (public blockchain). Experimental tests were conducted to measure the performance parameters under various loads of data and volume of transactions. Single-layer blockchain architectures were used as a control group so as to carry out a comparative analysis.

Research Choices

A single method quantitative option was made. Measures of quantitative nature like data processing speed, cost of data storage decrease, accuracy of security, rate of cyber-attacks and return on investment (ROI) were collected. The measures make it possible to compare and statistically justify the effectiveness of the system objectively.

Time Horizon

The study is carried out within cross-sectional time span when the information on the performance of the system were collected at a single time after the complete implementation of the prototype. It is a good form of experimenting the performance of architecture without temporal dependency.

Data Collection and Analysis

The main sources of data were the performance logs generated by the system and the security audit reports. percentage improvement, data benchmarking and indexes were used to carry out the data analysis. To have an integrated measure of assessment, an index of Hybrid Blockchain Effectiveness (HBEI) was developed, which was weighted on the benchmark of the security (0.40), scalability (0.30), data management (0.20), and interoperability (0.10) dimensions.

Ethical Considerations

The whole experimental information was generated in a virtual setting of the Internet of Things and no actual user information was exposed. The test had been conducted on ethical testing and had not done any unauthorized access on the external systems.

Results Analysis

System Processing Speed Performance

The first test was dedicated to the speed of the processing of data at the various loads of the IoT transactions. Isolated public and private blockchain systems were contrasted with the hybrid blockchain system. According to the findings, the proposed hybrid model has a large positive influence on the throughput because of the balance between on-chain verification and off-chain execution. The average processing rate of the hybrid system was 40 times higher than that of the public blockchain and 22 times higher than that of the private blockchain in moderate load conditions (5,000 transactions). This was improving with the increase in the volume of transaction and this means that it is scalable.

Table 4.1: Comparison of Data Processing Speed (%)

Architecture Type	Low Load	Medium Load	High Load
Public Blockchain	100%	100%	100%
Private Blockchain	118%	120%	122%
Hybrid Blockchain	135%	140%	142%

These findings confirm that hybrid blockchain systems effectively reduce validation bottlenecks, particularly under high-load IoT environments.

Storage Cost Efficiency Analysis

The optimisation of storage is an important issue in IoT ecosystems because data is constantly generated. The hybrid architecture stored most of the IoT data in off-chain storage and stored cryptographic hashes in chain storage. The findings indicate that cost of storage reduces by a factor of 30 against completely on-chain blockchain storage. The hybrid solution was still calculated to have a 20% lower cost when compared with centralized cloud storage with blockchain overlays as a result of less redundancy.

Table 4.2: Storage Cost Comparison (%)

Storage Model	Cost Index
Centralized Cloud Storage	100%
Public Blockchain Storage	138%
Private Blockchain Storage	115%
Hybrid Blockchain Storage	70%

This finding demonstrates the economic viability of large-scale IoT architectures based on a hybrid.

Data Authenticity and Integrity Results

The integrity and authenticity of data was tested by the rate of cryptographic verification of data in various architectures. The hybrid blockchain system had a data authenticity of 99.9 sergeant to both the public and the private blockchain system. The combination of unalterable proofs of ledgers and the management of private data became coordinated greatly minimizing the cases of tampering.

Table 4.3: Data Authenticity Accuracy (%)

Architecture	Authenticity Rate
Centralized System	92.5%
Public Blockchain	98.2%
Private Blockchain	97.6%
Hybrid Blockchain	99.9%

The findings reveal that hybrid blockchain frameworks provide better trust such assurance in data generated by IoT.

Cyber-Attack Reduction Performance

The evaluation of cybersecurity resilience was done by simulating typical attacks, such as replay attacks, unauthorized access, and data injection. The hybrid blockchain system reduced the successful cyber attacks by 95 percent as compared to centralized IoT systems. Attacks were lowered by 70 in public blockchain systems and 78 in private blockchains.

Table 4.4: Cyber-Attack Reduction Comparison (%)

System Type	Attack Reduction
Centralized IoT System	0%
Public Blockchain	70%
Private Blockchain	78%
Hybrid Blockchain	95%

This proves the appropriateness of hybrid authentication and the verification layers in enhancing the IoT security.

Scalability Under Increasing Device Density

Scalability testing was done by increasing the number of connected IoT devices and then 50,000. The performance of the hybrid blockchain architecture was not any different than the one of the public blockchains which had a latency increment of 38 per cent and the private blockchains which had a latency increment of 25 per cent.

Table 4.5: Latency Increase with Device Growth (%)

Number of Devices	Public	Private	Hybrid
1,000	0%	0%	0%
10,000	15%	10%	5%
25,000	28%	18%	9%
50,000	38%	25%	12%

The hybrid model is highly scalable, which can be used in the smart cities and industrial IoT worlds.

Interoperability and Network Integration

Success rates in cross-network data exchanges across the IoT platforms were one of the assessment criteria used to determine interoperability. The blockchain interoperability of the hybrid architecture was found to be 92 percentage (compared with the interoperability of the private blockchain 80 percent and the public blockchain 85 percent). The unified set of APIs and the cross-chain verification system made integration of the systems easier.

Table 4.6: Interoperability Performance (%)

Architecture	Interoperability Success
Public Blockchain	85%
Private Blockchain	80%
Hybrid Blockchain	92%

Such results imply the ability of the hybrid system to support nonhomogeneous IoT environments.

Hybrid Blockchain Effectiveness Index (HBEI)

To provide the consolidated analysis, the calculation of the weighted performance dimensions was performed to reflect Hybrid Blockchain Effectiveness Index (HBEI). The total HBEI score with the hybrid architecture of 0.91 would have been much higher than the public (0.68) and the private (0.74) blockchain systems.

Table 4.7: HBEI Comparison

Dimension	Weight	Public	Private	Hybrid
Security	0.40	0.26	0.30	0.38
Scalability	0.30	0.18	0.21	0.27
Data Management	0.20	0.14	0.15	0.18
Interoperability	0.10	0.10	0.08	0.08
Total HBEI	1.00	0.68	0.74	0.91

Return on Investment (ROI) Evaluation

According to the economic analysis, the hybrid blockchain architecture will generate a 4: 1 ROI, i.e., 1 unit of investment will generate four units of the value in terms of increased security, improved performance, and cost savings. PBSs had a 2:1 ROI in the public blockchain systems and 2.5:1 ROI in the private blockchain systems.

Table 4.8: ROI Comparison

Architecture	ROI Ratio
Public Blockchain	2:1
Private Blockchain	2.5:1
Hybrid Blockchain	4:1

This confirms the cost-efficiency of hybrid blockchain application in IoT implementations on a large scale.

Summary of Key Results

Overall, the hybrid blockchain system was observed to be better than the traditional system were all the dimensions in the test. The key findings are the 40 percent faster processing rate, 30 percent lower storage cost, and 99.9 percent authenticity of the data, 95 percent lower cyber-attacks, and scalability at the least increase in latency. Such results prove the effectiveness of the combination of the two layers blockchain (public and private) to handle the data of the IoT safely and in a large scale.

Discussion

The empirical evidence provided by the results of this paper offers immense support to the utility of hybrid blockchain architecture in addressing the long-lived challenges of security, scaling, and information control in the large-scale internet of things. The fact that the speed of the data processing increased by 40 times demonstrates that the use of both the public and the private blockchain layer may allow decreasing the quantity of the bottlenecks in the process of the transactions validation by a significant margin. It is particularly notable with regard to IoT ecosystems where real-time or near-real-time processing of data is required such as smart cities, industrial automation, and healthcare monitoring. The hybrid architecture offers a trade-off between the aspects of decentralization and efficiency in the sense that it distributes the computational load between the permissioned and permissionless ledgers.

The usefulness of the proposed method is also supported by the fact that storage is optimal. The benefit of off-chain data manipulation and on-chain integrity checks is emphasized by the decrease of the expenses applied in the storage by 30. This fact is in line with the earlier research that suggests that all-on-chain storage is not economical to support data-intensive IoT systems. The fact that the hybrid model can minimize redundancy by the same measure that it can ensure immutability shows that it may be employed to encourage long-term scalability and not expose it to excessive infrastructure.

Due to the security factor, the authenticity rate of the data of 99.9 percent and the 95 percent decrease in the successful cyber attacks implies that the system has considerably improved compared to the centralized and single layer blockchain system. The findings suggest that hybrid architectures can be used to overcome the common vulnerabilities of the IoT that include unauthorized access and altering information. The cryptographic validation and controlled access policies also offer a higher level of trust and flexibility in the operations, which otherwise would essentially be lacking in a strict implementation of a blockchain.

The other notable advantage on the hybrid approach is represented by scalability testing in the increased density of the devices. This is shown by the fact that, even the 12% reduction in latency at the higher device volumes is not huge, hence suggesting that, the architecture can scale to quick IoT with minimal performance degradation. This is required on emerging smart infrastructures that can grow exponentially in the number of devices in a relatively short period of time. In addition to it, 92% interoperability is a sign that the system can implement non-homogenous IoT sites, and permit data flow in a seamless way between networks.

All these performance improvements are summed up to one parameter of evaluative performance called the Hybrid Blockchain Effectiveness Index (HBEI) and the hybrid model scores 0.91, which is way higher than blockchain alternatives. This strength of systemic performance is transferred into the real economic returns, in the form of 4:1 payoff in investment. These general results indicate that hybrid blockchain models can offer an efficient, scalable, and cost-effective solution to ensure the security of IoT data management, which makes them one of the facilitators in the creation of digital infrastructure in the future.

Conclusion

The last section of this paper defends the opinion that is increasingly gaining traction and that hybrid blockchain systems represent a viable and quality method of secure and scalable IoT data management. The limitations associated with the existing blockchain and centralized system of IoT can be addressed with the proposed hybrid model that will be based on centralized efficiency and decentralized trust mechanisms. The processing speed, scalability, and data authenticity improvements obtained are consistent with the prior findings that reflect the productivity of hybrid authentication and access control systems in the heterogeneous IoT environment (Khashan and Khafajah, 2023; Pabitha et al., 2023).

The 99.9 percent data authenticity and 95 percent cyber-attack reduction, and scalability performance of the previous hybrid IoT blockchain research are also supported by empirical data stemming from the fact that more data layers result in greater resilience and performance (Sagirlar et al., 2018; Dhulavvagol et al., 2023). Additionally, the ability to provide low latency when scaling devices density enables the architecture to be deployed in massive applications of smart cities, healthcare, industrial internet of things, and so on (Jo et al., 2018; Agarwal and Pal, 2023).

In terms of strategy, the 4:1 of investment achieved in the course of this research will point to the fact that hybrid blockchain systems are not only technically viable, but they are also cost effective. This observation correlates with the recent literature that indicates cost-efficiency of the hybrid models in the creation of a balance between privacy, scalability, and operational efficiency (Banerjee et al., 2025; Lopez et al., 2024). In general, the study adds to the current literature in terms of quantitative validation of the hybrid block efficiency that could be used to justify systematic reviews and define hybrid-based architecture as the most promising way of the future solutions in the direction of security and data management of the IoT (Alkhateeb et al., 2022; Nandanwar and Katarya, 2025).

Recommendations

Based on the outcomes of this work, the following seven recommendations may be proposed to enhance the usability and effectiveness of hybrid blockchain systems to be applied in the management of IoT data:

Strategic Adoption of Hybrid Blockchain Architectures

Implementation of hybrid blockchain systems should be taken as a strategic move in the large-scale implementation of IoT systems within any organization so that the balance between decentralization and efficiency and security in operations is not lost. It can be scaled, and is more data-integrity aware, reducing transaction and infrastructure latency, and has been suitable in the smart city, healthcare, and industrial IoT applications.

2. Multi-Layered Security and Authentication Integration

Hybrid blockchain systems should have multi-layered security which includes blockchain based authentication systems, encryption and intrusion detection systems. Such integration would be extremely beneficial in safeguarding against cyber attacks, unauthorized entry, as well as ensuring the integrity of the data in heterogeneous networks of the IoT with minimal performance overhead.

3. Optimized Off-Chain and On-Chain Data Management

To solve this problem of storage, the data created by the IoT can be stored in off-chain repositories retaining cryptographic hash in the blockchain. Through this approach, storage redundancy is kept to a minimum, and system scalability can be improved as well as the data can be immutable, which is ensured to be cost-efficient in the long-term data-intensive IoT environments.

4. Standardization for Interoperability Enhancement

The developers and policymakers should promote standardized communication protocols, API and cross-chain interoperability frameworks. Such measures will be capable of facilitating effective data exchange between the various IoT systems and blockchain networks, improving the combination of the systems, reducing the complexity of the implementation, and maintaining the ecosystem of the heterogeneous systems.

5. Continuous Scalability and Performance Evaluation

It is advised to conduct regular performance testing as the density of the IoT devices grows in order to ensure the robustness of the system. Constant measurement allows exposing bottlenecks of latency, streamlining the consensus mechanisms, and ensuring price stability as IoT networks scale exponentially to various areas of application.

6. Comprehensive Cost–Benefit and ROI Assessment

Cost-benefit and return-on-investment analyses should be done on a periodic basis to assess the sustainability of infrastructure. The measurement of performance improvement, security enhancement, and operational benefits would contribute to the informed decision-making process and explain the necessity of further investment in hybrid blockchain-based IoT systems.

7. Future Integration with Emerging Technologies

The next generation applications should focus on the fusion of artificial intelligence, edge computing, and machine learning with hybrid blockchain architectures. This convergence may improve auto threat identification, smart resource distribution, and real-time decision making, and improve scalability, efficiency and security of next-generation IoT systems.

REFRENCES

Golder, S. S., Mondal, S., Das, S., Bose, R., Sutradhar, S., & Mondal, H. (2024, December). Hybrid Blockchain Framework for Secure and Scalable Internet of Things (IoT) Networks (HB-IoT): A Novel Approach. In 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA) (pp. 1-7). IEEE.

Sharmin, S., Arefin, M. S., Dhar, P. K., Sultana, Z., & Akter, S. (2025). A Scalable and Privacy-Preserving Hybrid Blockchain Architecture for Secure Healthcare Data Management. International Journal of Advanced Computer Science & Applications, 16(8)

Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T. T., Assam, M., ... & Mohamed, H. G. (2023). Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning. Sensors, 23(18), 7740.

Haque, E. U., Shah, A., Iqbal, J., Ullah, S. S., Alroobaea, R., & Hussain, S. (2024). A scalable blockchain based framework for efficient IoT data management using lightweight consensus. Scientific Reports, 14(1), 7841.

Irshad, R. R., Hussain, S., Hussain, I., Nasir, J. A., Zeb, A., Alalayah, K. M., ... & Alwayle, I. M. (2023). IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing. IEEE Access, 11, 105479-105498.

Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., ... & Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. Alexandria Engineering Journal, 65, 263-274.

Lee, C., Kim, J., Ko, H., & Yoo, B. (2024). Addressing IoT storage constraints: A hybrid architecture for decentralized data storage and centralized management. Internet of Things, 25, 101014.

Khashan, O. A., & Khafajah, N. M. (2023). Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. Journal of King Saud University-Computer and Information Sciences, 35(2), 726-739.

Massan, S. U. R., Wagan, A. I., & Shaikh, M. M. (2020). A new metaheuristic optimization algorithm inspired by human dynasties with an application to the wind turbine micrositing problem. Applied Soft Computing, 96, 106618. https://doi.org/10.1016/j.asoc.2020.106618

Pabitha, P., Priya, J. C., Praveen, R., & Jagatheswari, S. (2023). Modchain: a hybridized secure and scaling blockchain framework for iot environment. International Journal of Information Technology, 15(3), 1741-1754.

Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J. D., & Ragnoli, E. (2018, July). Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1007-1016). IEEE.

Banerjee, D., Sharma, J., Chilluri, V. S. B., Yang, T., Wang, L., & Rathore, R. S. (2025, March). A Hybrid Blockchain Framework for Securing Healthcare Data: Balancing Privacy and Scalability. In International Conference on Computing and Communication Systems for Industrial Applications (pp. 229-238). Singapore: Springer Nature Singapore.

Dhulavvagol, P. M., Prasad, M. R., Kundur, N. C., Jagadisha, N., & Totad, S. G. (2023). Scalable blockchain architecture: leveraging hybrid shard generation and data partitioning. International Journal of Advanced Computer Science and Applications, 14(8).

Jo, B. W., Khan, R. M. A., & Lee, Y. S. (2018). Hybrid blockchain and internet-of-things network for underground structure health monitoring. Sensors, 18(12), 4268.

Agarwal, V., & Pal, S. (2023). HierChain: A hierarchical-blockchain-based data management system for smart healthcare. IEEE Internet of Things Journal, 11(2), 2924-2934.

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. Sensors, 22(4), 1304.

Lopez, L. J. R., Millan Mayorga, D., Martinez Poveda, L. H., Amaya, A. F. C., & Rojas Reales, W. (2024). Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review. Computers, 13(6), 152.

Nandanwar, H., & Katarya, R. (2025). A hybrid blockchain-based framework for securing intrusion detection systems in internet of things. Cluster Computing, 28(7), 471.

Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15), 9711-9733.

Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and distributed computing, 164, 152-167.

Zhou, E., Hong, Z., Xiao, Y., Zhao, D., Pei, Q., Guo, S., & Akerkar, R. (2022). MSTDB: A hybrid storage-empowered scalable semantic blockchain database. IEEE Transactions on Knowledge and Data Engineering, 35(8), 8228-8244.

Khan, A. A., Laghari, A. A., Alroobaea, R., Baqasah, A. M., Alsafyani, M., Alsufyani, H., & Ullah, S. (2025). A lightweight scalable hybrid authentication framework for Internet of Medical Things (IoMT) using blockchain hyperledger consortium network with edge computing. Scientific Reports, 15(1), 19856.

Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, 650-655.

Nuthalapati, A. (2023). Building scalable data lakes for Internet of Things (IoT) data management. Educational Administration: Theory and Practice, 29(1), 412-424.

Dhruvitkumar, V. T. (2021). Scalable AI and data processing strategies for hybrid cloud environments.

Agrawal, R., Singhal, S., & Sharma, A. (2024). Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. Cluster computing, 27(6), 8015-8030.