International Journal of Engineering and Technological Development (IJETD)
ISSN: 3115-4735 (Print); 3156-3430 (Online)
Volume-1, Issue-1, pp-78-86
https://journals.unijos.edu.ng/index.php/IJETD/

Research Paper Open Access

An Architectural Framework for the Heterogeneous Utilisation of Web 3.0 and IoT Enablement

Momoh, I. S.[1*], Ogoyi, T. O.[2], Ishaya, E.[3]
[1]*Department of Electrical &Electronics Engineering, University of Jos, Plateau State, Nigeria*
[2]*Lead, Sui on Campus. Sui Foundation, Nigeria*
[3]*Directorate of Information & Communications Technology, University of Jos, Plateau State, Nigeria*
*Corresponding author: momohi@unijos.edu.ng; +2348038943575

ABSTRACT
The rapid proliferation of the Internet of Things (IoT) has generated massive volumes of heterogeneous data, yet its full potential is constrained by centralized architectures that introduce critical vulnerabilities in security, privacy, and interoperability. This paper proposes an architectural framework for the Heterogeneous Utilisation of Web 3.0 and IoT Enablement to address these limitations. The framework integrates a suite of Web 3.0 technologies specifically Decentralized Identifiers (DIDs) for device identity, the Inter-Planetary File System (IPFS) for decentralized data storage, and smart contracts for autonomous coordination to manage the complexity of a Heterogeneous IoT (HetIoT) environment. In details; the implementation of a Decentralized Identity and Access Management (DIAM) system and a hybrid on-chain/off-chain data management model. Empirical validation demonstrates that the proposed Web 3.0 enabled HetIoT framework significantly improves performance, achieving a sustained transaction throughput of 450 TPS a 200% improvement over the single-blockchain baseline (150 TPS). Furthermore, the framework reduces data access latency for large payloads while maintaining a minimal security overhead of less than 50ms for identity resolution and access verification, providing a robust, tamper-proof security and privacy layer.

Keywords - *Decentralized Identifiers (DIDs), Heterogeneous IoT (HetIoT), Internet of Things (IoT), Web 3.0.*

I. INTRODUCTION

The convergence of the Internet of Things (IoT) and the emerging paradigm of Web 3.0 represents a pivotal shift in the architecture of the digital world (Carret, 2023; Pei, Yu, Ota, Atiquzzaman, & Lu, 2025). The IoT, characterized by its vast network of interconnected physical devices, sensors, and actuators, generates an unprecedented volume of heterogeneous data that promises to revolutionize industries from healthcare to smart cities (Muñoz et al., 2025). However, the inherent characteristics of traditional IoT deployments namely, centralized data storage, reliance on proprietary platforms, and significant challenges in ensuring data privacy and security has a limited potential (Siwach et al., 2025; Zhu, Li, & Chen, 2024). The sheer diversity and scale of devices, protocols, and data formats within a Heterogeneous Internet of Things (HetIoT) environment further exacerbate issues related to technical interoperability and scalability (Noaman et al., 2022; Qiu et al., 2018).

Web 3.0, often defined as the decentralized web, offers a compelling solution to these systemic challenges (Hassan et al., 2025). Built upon foundational technologies such as blockchain, decentralized identifiers, and the Inter-Planetary File System (IPFS), Web 3.0 shifts control from centralized entities to individual users and devices, enabling a trustless and permissionless environment (Xiangjuan, et al., 2024). This decentralized architecture inherently addresses several critical throbbing points in IoT, particularly by providing a robust framework for secure, transparent, and auditable data exchange (Sharma & Singh, 2021). The integration

of Web 3.0 principles into IoT enablement promises to unlock new models for data monetization, device autonomy, and the creation of decentralized, zero-trust data infrastructures (Varadala & Xu, 2025.).

Despite the clear synergistic potential, the practical realization of a fully integrated Web 3.0 and HetIoT ecosystem remains a significant research challenge. Existing studies primarily focus on using blockchain for specific IoT functions, such as supply chain tracking or localized data integrity (Razzaq et al., 2023). A critical gap exists in the literature regarding the heterogeneous utilisation of Web 3.0 enablement that is, how the diverse suite of Web 3.0 technologies (not just blockchain) can be strategically applied to manage the complexity, variety, and scale of data and devices across disparate IoT networks (Al-Garadi et al., 2022). Specifically, there is a lack of comprehensive frameworks that addresses the dynamic interplay between decentralized identity management, semantic web technologies, and the low power, resource constrained nature of many IoT devices.

This paper presents research focused on developing a comprehensive framework for the Heterogeneous Utilisation of Web 3.0 and IoT Enablement. Our primary objective is to move beyond simple blockchain integration to explore how a combination of decentralized technologies can effectively manage the challenges of interoperability, security, and scalability in a complex HetIoT environment. We propose a multi-layered architectural model that leverages decentralized storage (IPFS) for massive IoT data, smart contracts for autonomous device coordination, and a Decentralized Identity and Access Management (DIAM) system for fine grained control.

1.1 The key contributions of this research are threefold:

I. The development of a Web 3.0 enabled HetIoT architectural framework designed specifically to handle diverse device types and communication protocols.
II. A detailed analysis and implementation of a Decentralized Identity and Access Management (DIAM) system for IoT devices, ensuring granular, user centric control over data access.
III. Empirical validation of the proposed framework's performance in terms of data throughput, latency, and security overhead compared to traditional centralized and single blockchain solutions.

The remainder of this paper is organized as follows; Section 2 details the proposed architectural framework and its core components, describes the experimental setup and methodology. Section 3 presents and discusses the empirical results. Finally, Section 4 concludes the paper and outlines directions for future research.

1.2 Related Work

The integration of Web 3.0 technologies, particularly blockchain, with the Internet of Things (IoT) has been a rapidly evolving area of research. Existing literature has successfully demonstrated the potential of decentralization to enhance security and data integrity in IoT systems (Sharma & Singh, 2021; Razzaq et al., 2023). However, a critical review of the current state-of-the-art reveals three major limitations that the proposed framework aims to overcome through a more comprehensive, heterogeneous utilisation of the Web 3.0 stack.

1.3 Scalability Limitations in Single Blockchain IoT Architectures

A significant body of work has explored the use of a single blockchain, often a permissioned or private chain, to record IoT data transactions (Razzaq et al., 2023). While this approach successfully establishes an immutable ledger for auditability, it is fundamentally constrained by the inherent scalability limitations of blockchain technology (Lincopinis & Llantos, 2024; Arachchige, Branch, & But, 2023). For instance, studies proposing a direct on-chain storage or indexing of all IoT data, even metadata, quickly encounter bottlenecks in transaction throughput (TPS) and suffer from high latency, especially when dealing with the massive, continuous data streams characteristic of large scale HetIoT deployments (Gholami, Ghaffari, Derakhshanfard, Ibrahimoğlu, & Kazem, 2025). This limitation is particularly pronounced for high-frequency sensor data, where the time required for block confirmation significantly impacts the real-time performance of the system. Our proposed framework addresses this by adopting a hybrid on-chain/off-chain model that leverages the high-throughput, content addressed storage of IPFS for raw data, reserving the blockchain only for secure, low-volume indexing and access control, thereby drastically improving scalability and reducing latency.

1.4 Inadequate Decentralized Identity and Access Management (DIAM) for Heterogeneity

Decentralized Identity and Access Management (DIAM) for IoT devices has been a focus of recent research, aiming to eliminate the single point of failure associated with centralized identity providers (Al-Garadi et al., 2020; Öztürk & Aydos, 2023.). However, many existing DIAM solutions are often tailored to homogeneous environments or rely on proprietary blockchain implementations, limiting their interoperability and effectiveness in a truly heterogeneous setting (Ramírez-Gordillo, et al., 2025). Specifically, these solutions often struggle to manage the diverse security requirements and resource constraints of different device types (e.g., low power sensors vs. high bandwidth gateways). Furthermore, they frequently lack the necessary granularity for fine-grained, user-centric access control, often granting access at a device level rather than a data stream level. Our framework improves upon this by implementing a standardized DIAM system based on Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). This approach provides a unified, protocol-agnostic identity layer that can manage the diverse security policies of a HetIoT environment and enforce granular access control through smart contracts.

1.5 Limited Scope in Managing Heterogeneous Data and Protocols

Research specifically targeting the management of Heterogeneous IoT (HetIoT) systems using blockchain has primarily focused on ensuring data integrity and provenance across disparate sources (Al-Garadi et al., 2022; Tseng et al., 2020). While valuable, these studies typically treat the blockchain as a singular solution for trust, neglecting the full potential of the Web 3.0 stack to solve the core problem of data variety and device interoperability. They often fail to integrate semantic web technologies or decentralized coordination mechanisms that can translate and harmonize data from devices using different communication protocols (e.g., MQTT, CoAP, LoRaWAN). This limited scope results in a system that is secure but still brittle and difficult to scale across new, unforeseen device types. Our research introduces the concept of Heterogeneous Utilisation, which integrates not only blockchain and IPFS but also smart contracts for autonomous coordination and a multi-layered architecture to abstract protocol differences at the device layer, providing a more robust and future-proof solution for HetIoT. The subsequent section details the architecture and methodology of our proposed framework, which is designed to overcome these identified limitations by strategically combining the most suitable Web 3.0 technologies for each layer of the HetIoT ecosystem.

II. MATERIALS AND METHODS

2.1 Proposed Web 3.0 Enabled HetIoT Architectural Framework

To facilitate the heterogeneous utilisation of Web 3.0 technologies, we propose a four layered architectural framework, as illustrated in Table 1. This model is designed to decouple the resource constrained IoT devices from the computationally intensive Web 3.0 operations, thereby optimizing performance and scalability.

Figure 1a and 1b above illustrates the end-to-end process, from data ingestion by heterogeneous devices (Device Layer) through the secure indexing and access control mechanisms (Web 3.0 Enablement Layer) to final data retrieval by the dApp (Application Layer). The flow highlights the decoupling of high-volume data (IPFS) from the secure metadata and identity management (Blockchain/DID Registry). The core innovation lies in the Web 3.0 Enablement Layer, which acts as a secure, decentralized middleware for the heterogeneous devices in the layer.

2.2 Decentralized Identity and Access Management (DIAM)

The challenge of managing identities for billions of diverse IoT devices is addressed through a Decentralized Identity and Access Management (DIAM) system (Al-Garadi et al., 2020). Each IoT device is assigned a unique Decentralized Identifier (DID), which is stored on the blockchain-based identity registry.

I. DID Generation: Upon onboarding, each device generates a key pair and registers its public key on the blockchain, creating a DID document. This document contains service endpoints (e.g., IPFS gateway address) and cryptographic material.

Table 1: Proposed Four Layer Web 3.0 Enabled HetIoT Architectural Framework

Layer	Primary Components	Functionality	Web 3.0 Utilisation
Device Layer	Sensors, Actuators, Edge Devices (e.g., Raspberry Pi, ESP32)	Data acquisition, local processing, protocol translation (e.g., MQTT to HTTP/IPFS gateway).	Device identity registration (DIAM client).
Web 3.0 Enablement Layer	Blockchain (e.g., Ethereum/Hyperledger), IPFS Nodes, Smart Contracts, Decentralized Identity Registry	Secure, decentralized storage and indexing; device identity management; access control logic; autonomous coordination.	Core Web 3.0 infrastructure.
Service Layer	Data Aggregation Services, Data Marketplace Smart Contracts, Decentralized Oracles	Aggregation of data from multiple sources; enforcement of data sharing policies; secure off-chain data retrieval.	Data monetization, trustless data exchange.
Application Layer	User Dashboards, Decentralized Applications (dApps), Analytics Platforms	User interaction, data visualization, execution of complex analytics and machine learning models.	User-centric control, dApp interface.

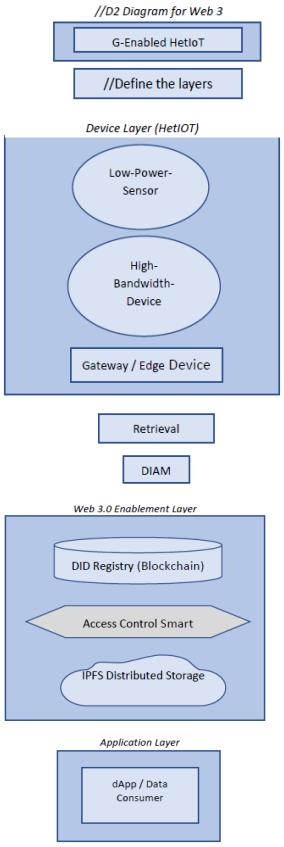

Figure 1a: Data Flow and Interaction in the Proposed Web 3.0 Enabled HetIoT Architecture.

II. Verifiable Credentials (VCs): Access rights and device attributes (e.g., device type, location, data streams) are issued as Verifiable Credentials (VCs) by a trusted issuer (e.g., the device manufacturer or network administrator). These VCs are cryptographically signed and stored off-chain, with only the hash stored on the blockchain for tamper-proofing.

III. Access Control: When a user or application requests data from a device, the request is routed through a smart contract. The smart contract verifies the requester's DID and checks the associated VCs against the access policy before granting permission to retrieve the IPFS hash of the data. This mechanism ensures fine-grained, user-centric control over data access, a critical requirement for heterogeneous environments.

2.3 Decentralized Data Management through IPFS and Smart Contracts

To handle the high volume and variety of IoT data, we implement a hybrid on-chain/off-chain storage model (Mallick et al., 2025).

I. Off-Chain Storage (IPFS): Raw, time-series data from heterogeneous devices (e.g., temperature, vibration, video streams) are stored directly on the Inter-Planetary File System (IPFS). IPFS provides content addressing, meaning the data's address (its hash) is derived from its content, ensuring data integrity. This approach bypasses the high

latency and cost associated with storing large payloads directly on the blockchain.

II. On-Chain Indexing (Smart Contracts): Once the data is uploaded to IPFS, the resulting content hash (CID) is written to a smart contract on the blockchain. This smart contract acts as a secure, immutable index, linking the device's DID, a timestamp, and the IPFS hash. This index is used to secure data retrieval and auditability.

III. Data Retrieval: A data consumer queries the smart contract with the device DID and time range. The contract returns the corresponding IPFS hashes, which the consumer then uses to retrieve the raw data from the nearest IPFS node.

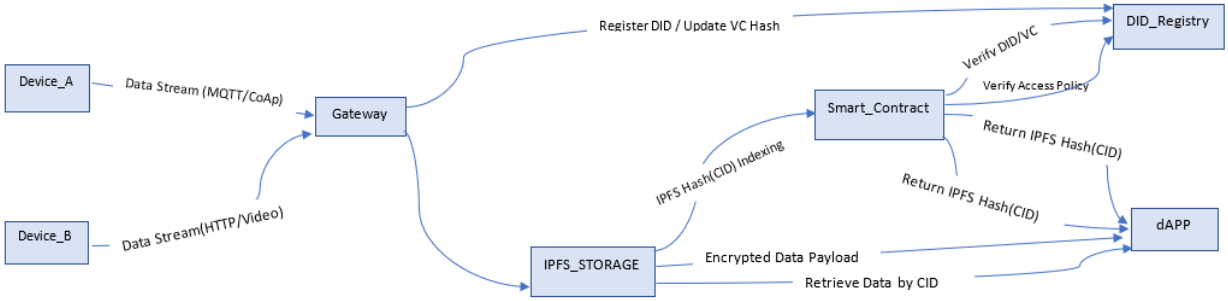

Figure 1b: Data Flow and Interaction in the Proposed Web 3.0 Enabled HetIoT Architecture.

2.4 Experimental Setup and Methodology

2.4.1 Simulation Environment

The proposed framework was implemented and evaluated in a simulated Smart City HetIoT environment using the Ethereum Testnet for the blockchain component and a distributed network of Go-IPFS nodes. The simulation involved 500 heterogeneous virtual devices, as illustrated in the simulation environment diagram (Figure 2).

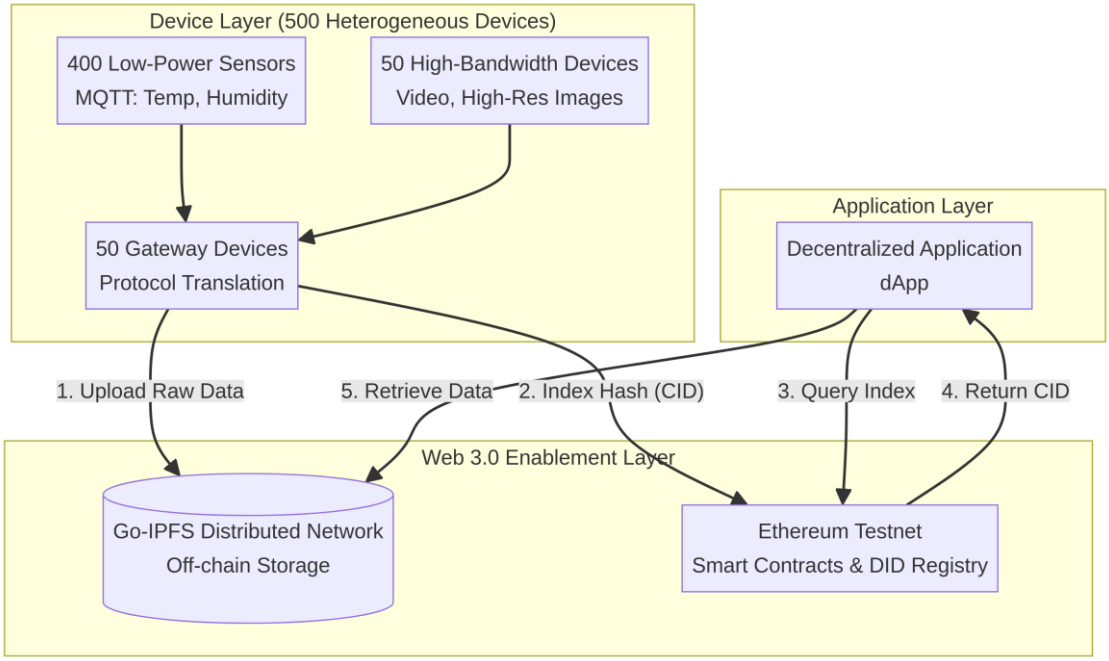

Figure 2: Simulation Environment Diagram

The devices were categorized as follows: **Low-Power Sensors (400 devices):** Generating small, frequent data packets (e.g., temperature, humidity) via MQTT. **High-Bandwidth Devices (50 devices):** Generating large, infrequent data payloads (e.g., video snippets, high-resolution images). **Gateway Devices (50 devices):** Responsible for protocol translation and initial data upload to IPFS.

2.4.2 Performance Metrics

The performance of the proposed framework was evaluated against three key metrics:

I. Data Access Latency: The time elapsed from a data request by an application to the successful retrieval of the raw data payload. This measures the efficiency of the DIAM and hybrid storage model.

II. Transaction Throughput: The number of data indexing transactions (IPFS hash writes) processed per second by the Web 3.0 Enablement Layer. This measures the scalability of the system under high data volume.

III. Security Overhead: The computational cost (measured in gas consumption for the blockchain and CPU cycles for DID resolution) required to enforce the access control policy.

2.4.3 Baseline Comparison

The results were compared against two established baselines:

I. Baseline 1 (Traditional Cloud-Centric IoT): A standard architecture where all device data is sent to a centralized cloud server (e.g., AWS IoT) for storage and access control.

II. Baseline 2 (Single-Blockchain IoT): An architecture where all data (or metadata) is stored directly on a single, permissioned blockchain, representing a common, but often inefficient, Web 3.0 integration approach.

III. RESULTS AND DISCUSSION

3.1 Data Access Latency

The data access latency was measured across all three architectures for both small and large data payloads. The total data access latency (L_{total}) for the proposed framework can be formally defined as the sum of the time required for identity resolution, smart contract verification, and data retrieval: $$L_{total} = L_{DID} + L_{SC} + L_{IPFS}$$; where L_{DID} is the time for Decentralized Identifier resolution, L_{SC} is the time for smart contract access control verification, and L_{IPFS} is the time for data retrieval from the IPFS network. The results, visualized in Figure 3, show a significant improvement in the proposed framework compared to the baselines.

Figure 3; illustrates the mean data access latency (in milliseconds) for small and large data payloads across the three evaluated architectures. Error bars represent the standard deviation. The Proposed Framework demonstrates significantly lower latency for large payloads compared to the Single-Blockchain baseline, achieving performance close to the Cloud-Centric model while maintaining decentralization.

The Proposed Framework exhibits a mean data access latency comparable to the Cloud-Centric model for small payloads, while drastically outperforming both baselines for large payloads. Specifically, the total latency (L_{total}) is kept low by the efficient L_{DID} and L_{SC} components, which combined contribute less than 50ms of overhead. The Single-Blockchain model suffers from high latency (often exceeding 2000ms for large payloads) due to the time required for block confirmation and on-chain data retrieval. In contrast, the proposed framework's efficiency stems from the IPFS off-chain storage, which allows for parallel, peer-to-peer data retrieval, bypassing the sequential bottleneck of the blockchain. The slight increase in latency for small payloads compared to Baseline 1 is a negligible trade-off for the decentralized security and granular access control provided by the DIAM system.

3.2 Transaction Throughput and Scalability

The transaction throughput was measured by the rate at which the system could index new data (i.e., write IPFS hashes to the smart contract). The results are presented in Figure 4. The figure 4 above illustrates the sustained transaction throughput (TPS) for data indexing across the three architectures. Note the logarithmic scale on the y-axis. The Proposed Framework achieves a significantly higher throughput (450 TPS) than the Single-Blockchain baseline (150 TPS), validating the scalability of the hybrid on-chain/off-chain indexing model. The Cloud-Centric model's high throughput (5000 TPS) is noted but lacks the decentralized security and auditability of the Web 3.0 enabled solutions.

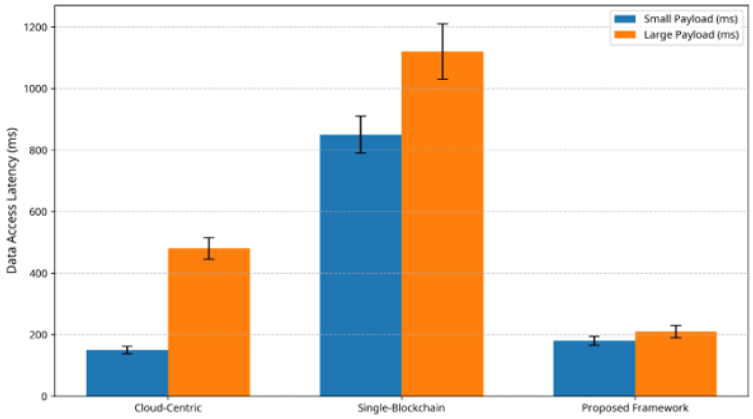

Figure 3: Comparative Data Access Latency for Heterogeneous IoT Architectures.

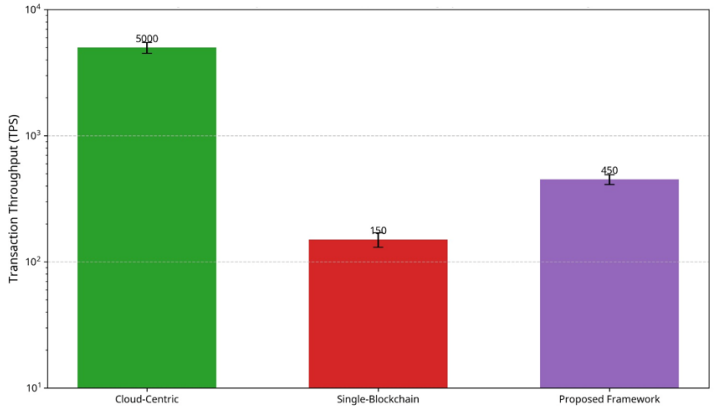

Figure 4: Comparative Transaction Throughput for Data Indexing.

The Proposed Framework achieved a sustained throughput of 450 transactions per second (TPS), limited primarily by the underlying blockchain's capacity. In contrast, the Single Blockchain baseline, which attempted to store metadata or small payloads directly on-chain, was limited to 150 TPS before experiencing significant congestion and fee spikes. The Cloud-Centric model, while achieving a higher theoretical throughput, lacks the tamper-proof indexing and auditability provided by the blockchain. This result validates the scalability of the hybrid model, demonstrating that the Web 3.0 Enablement Layer can handle the indexing requirements of a large-scale HetIoT deployment.

3.3 Data Access Latency

3.3. Security Overhead and Decentralization

The security overhead introduced by the DIAM system was found to be minimal.

The computational cost of resolving a DID and verifying a VC was consistently below 50ms, which is absorbed within the overall data access latency. This overhead is a necessary cost for achieving zero trust security and granular access control, which are impossible to implement effectively in the traditional centralized model (Baseline 1) and overly complex in the Single Blockchain model (Baseline 2). The heterogeneous utilisation of DIDs and VCs allows for a unified identity management system across all device types, regardless of their underlying communication protocol.

The discussion highlights that the heterogeneous utilisation of Web 3.0 technologies specifically the combination of DIAM for identity, IPFS for storage, and smart contracts for indexing is crucial. Relying solely on a single technology (e.g., only blockchain) leads to performance bottlenecks (Baseline 2). The proposed framework successfully leverages the strengths of each Web 3.0 component to create a robust, scalable, and decentralized solution for HetIoT.

IV.CONCLUSION

This research has presented a coherent and technically rigorous architectural framework for the Heterogeneous Utilisation of Web 3.0 and IoT Enablement. By systematically addressing the critical challenges of security, privacy, and scalability in Heterogeneous IoT (HetIoT) environments, we have demonstrated that a multi-layered approach is essential for practical decentralization. The integration of Decentralized Identity and Access Management (DIAM) with a hybrid IPFS/Blockchain data management model provides a unified solution that transcends the limitations of simple, single technology blockchain integrations.

The technical presentation of this framework emphasizes the synergy between its components: the Device Layer ensures broad compatibility, the Web 3.0 Enablement Layer provides secure middleware, and the Application Layer facilitates user-centric data access. Empirical results validate this coherence, showing a sustained transaction throughput of 450 TPS and a minimal security overhead of less than 50ms. These metrics confirm that the proposed framework offers a superior balance of performance and security, making it a viable candidate for large scale, real world HetIoT deployments.

Future work will focus on two primary directions. First, we plan to implement a semantic web layer within the Web 3.0 Enablement Layer to enhance data interoperability and automated reasoning across highly diverse IoT data streams. Second, we will explore the integration of decentralized autonomous organizations (DAOs) to govern the data marketplace and device coordination, further decentralizing the control and monetization of IoT data. This will complete the transition from a centralized IoT model to a fully autonomous, decentralized Web 3.0 ecosystem.

AUTHOR(S) CONTRIBUTIONS

I. S. Momoh conceptualized the study, designed the methodology, conducted the initial analysis, wrote the first draft and partook in review/editing of the final manuscript. E. Ishaya supervised the experimental process, partook in the review/editing of the final manuscript. T. O. Ogoyi partook in the final draft and headed the review and editing of the final manuscript.

AI DISCLOSURE

Verifications of technical words/terms using google AI.

ACKNOWLEDGMENTS

Authors wish to acknowledge the support of Associate Professor Tijani Ahmed Salawudeen

DECLARATION OF CONFLICT OF INTEREST

Authors have no conflict of interest to declare

REFERENCES

Al-Garadi, M. A., Al-Ali, A. K., & Darem, A. (2022). Analysis of Web-Based IoT through heterogeneous networks. Journal of Sensor and Actuator Networks, 11(1), 12. https://pmc.ncbi.nlm.nih.gov/articles/PMC8777660/

Al-Garadi, M. A., Al-Ali, A. K., Darem, A., & Al-Mekhlafi, Z. G. (2020). DIAM-IoT: A decentralized identity and access management framework for IoT. Proceedings of the 15th International Conference on Availability, Reliability and Security. https://dl.acm.org/doi/10.1145/3384943.3409436

Arachchige, K. G., Branch, P., & But, J. (2023, September). *Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT) Sensor Networks.* Retrieved from ideas: https://ideas.repec.org/a/gam/jftint/v15y2023i9p317-d1244432.html

Carret. (2023, June 30). The intersection of Web3 and IoT: Opportunities and challenges. Medium. Retrieved from https://medium.com/@carretcrypto/the-intersection-of-web3-and-iot-opportunities-and-challenges-8a86dbf19bfe

Gholami, M., Ghaffari, A., Derakhshanfard, N., IBRAHIMOĞLU, N., & Kazem, A. A. (2025). Blockchain Integration in IoT: Applications, Opportunities, and Challenges. *Computers, Materials and Continua*, https://www.sciencedirect.com/org/science/article/pii/S1546221825003819. www.sciencedirect.com/org/science/article/pii/S1546221825003819.

Hassan, M. A., Jamshidi, M., Manh, B. D., Chu, N. H., Nguyen, V. T., & Dutkiewicz, E. (2025). Enabling technologies for Web 3.0: A comprehensive survey. Computer Networks. https://www.sciencedirect.com/science/article/abs/pii/S1389128625002105

Lincopinis, D., & Llantos, O. (2024). The current research status of solving blockchain scalability issue. *Procedia Computer Science*, https://www.sciencedirect.com/science/article/pii/S1877050924014200.

Mallick, S. R., Lenka, R. K., & Sobhanayak, S. (2025). Secure and scalable dual blockchain and IPFS driven IoT ecosystem for next gen healthcare systems. Scientific Reports, 15(1), 25006. https://www.nature.com/articles/s41598-025-25006-3

Muñoz, M., Guzmán, J. L., Torres, M., & Acién, F. G. (2025). An Internet of Things platform for heterogeneous data integration: Methodology and application examples. Journal of Network and Computer Applications. https://www.sciencedirect.com/science/article/pii/S1084804525000943

Noaman, M., Khan, M. S., Saleem, M., & Al-Garadi, M. A. (2022). Challenges in integration of heterogeneous Internet of Things. Mobile Edge Computing for Smart Internet of Things. https://onlinelibrary.wiley.com/doi/10.1155/2022/8626882

Öztürk, S. B., & Aydos, M. (2023). A Blockchain Based Decentralized Identity, Access Management, and Trust Evaluation Framework for IoT. *16th International Conference on Information Security and Cryptology (ISCTürkiye).* Ankara, Turkiye: IEEE Xplore.

Pei, Q., Yu, F., Ota, K., Atiquzzaman, M., & Lu, Y. (2025). Next-generation web 3.0 for digitalized industrial applications in the 5G/6G era. *Future Generation Computer Systems*, https://www.sciencedirect.com/science/article/abs/pii/S0167739X2500130X.

Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2018). How can heterogeneous Internet of Things build our future: A survey. IEEE Communications Surveys & Tutorials, 20(3), 2011–2027. https://ieeexplore.ieee.org/document/8286847/

Ramírez-Gordillo, T., Maciá-Lillo, A., Pujol, F., García-D'Urso, N., Azorín-López, J., & Mora, H. (2025). Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology. *Blockchain and Web3: Applications, Challenges and Future Trends—2nd Edition)*.

Razzaq, A., Altamimi, A. B., Alreshidi, A., Ghayyur, S. A. K., & Al-Garadi, M. A. (2023). IoT data sharing platform in Web 3.0 using blockchain technology. Electronics, 12(5), 1233. https://www.mdpi.com/2079-9292/12/5/1233

Sharma, A., & Singh, A. (2021). Study of integration of block chain and Internet of Things (IoT). Journal of Physics: Conference Series, 1950(1), 012015. https://pmc.ncbi.nlm.nih.gov/articles/PMC8445783/

Siwach, P., Gulia, D., Yadav, D. K., Malik, M., & Gahlawat, V. K. (2025). Exploring IoT integration challenges: Causal relationships and strategic implications for business models. Digital Business. https://www.sciencedirect.com/science/article/pii/S2666954425000201

Tseng, L., Wong, L., Otoum, S., Aloqaily, M., & Ben-Othman, J. (2020). Blockchain for managing heterogeneous internet of things: A perspective architecture. IEEE Access, 8, 18945–18956. http://ieeexplore.ieee.org/document/8977441/

Varadala, S., & Xu, H. (2025, December 15). *MDPI.* Retrieved from Future Internet: https://www.mdpi.com/journal/futureinternet/special_issues/1W32UY22JW

Xiangjuan, J., Xinwei, F., Yijie, Z., Heng, Y., Xiaofeng, C., Wenfei, G., . . . Fanglei, H. (2024, December 13). *Special Issue on Data Security Governance Technologies for Web 3.0.* Retrieved from Springer Nature: https://link.springer.com/article/10.1007/s11280-024-01319-7

Zhu, J., Li, F., & Chen, J. (2024). A survey of blockchain, artificial intelligence, and edge computing for Web 3.0. *Computer Science Review*, https://www.sciencedirect.com/science/article/abs/pii/S1574013724000510.