Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 7, pp. 2875–2888
DOI : 10.47974/JDMSC-2558

Comparative analysis of a novel smart contract-based hybrid access control model for blockchain-enabled secure IoT home automation systems

Abhishek Dadhich *
Bright Keswani †
Department of Computer Science & Engineering
Poornima University
Jaipur 303905
Rajasthan
India

Dinesh Goyal §
Department of Computer Science & Engineering
Poornima Institute of Engineering and Technology
Jaipur 302022
Rajasthan
India

Abstract

The rapid growth of Internet of Things (IoT)-enabled smart home environments has amplified the need for robust, scalable, and context-aware access control mechanisms. Traditional Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) models offer distinct advantages such as hierarchical simplicity and contextual granularity, respectively, yet exhibit critical limitations when deployed in isolation. To address these constraints, this study proposes and implements a discrete, hybrid RBAC–ABAC access control framework, engineered as a smart contract on the Binance Smart Chain (BSC), to ensure a secure, decentralized model for managing access to IoT resources. The framework leverages blockchain's inherent strengths cryptographic integrity, immutable message digests, and tamper-resistant audit trails to reinforce data confidentiality and policy enforcement. Validated on a real-world testbed comprising ESP32-based IoT devices, a Raspberry Pi gateway, and a blockchain backend, the proposed system demonstrates enhanced resilience and trust. Quantitative evaluations benchmark the hybrid model against standalone RBAC

* *E-mail:* 2021phdoddabhishek9333@poornima.edu.in (Corresponding Author)
† *E-mail:* bright.keswani@poornima.edu.in
§ *E-mail:* dinesh8dg@gmail.com

and ABAC mechanisms across key metrics, including gas consumption, access latency, access decision accuracy, and scalability. The results indicate the hybrid model achieves superior accuracy (97.2%) and scalability (supporting 50 concurrent users and 30 devices), with moderate gas usage (15,000 gwei) and acceptable latency (1.8 seconds). Furthermore, the use of laser-secure transaction protocols and cryptographic primitives within the smart contract enhances the protection of access rights and resource interactions. This hybrid smart contract architecture not only bridges the gap between theoretical access control models and practical blockchain deployments but also sets a foundation for adaptive, secure, and decentralized policy enforcement in next-generation smart homes, particularly in resource-constrained environments.

Subject Classification: *68M14, 68M20, 68M25, 68M32, 94A60.*

Keywords: *Hybrid access control, Blockchain-enabled smart homes, Smart contracts, IoT security, Comparative performance evaluation.*

1. Introduction

Traditional centralized architectures suffer from single points of failure, potential data manipulation, and privilege misuse, underscoring the necessity for robust, context-aware access control mechanisms in smart home systems [1]. Specifically, smart contracts serve as immutable, tamper-resistant replacements for centralized access servers by embedding access control logic directly into programmable blockchain code [5], [6]. These contracts utilize message digest techniques for verifiable state transitions and provide automated, auditable enforcement of access policies [2]. Among blockchain platforms, Binance Smart Chain (BSC) stands out due to its low-latency finality (~3 seconds), minimal transaction fees, and full compatibility with Ethereum's Solidity language, real-time access control in resource-constrained IoT environments. Access control frameworks commonly rely on Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). RBAC defines access permissions based on user roles (e.g., admin, guest), facilitating administrative efficiency and hierarchical policy enforcement, yet lacks sensitivity to contextual attributes like device type or user location [4], In contrast, ABAC allows for highly expressive, fine-grained policies by incorporating user, resource, and environmental attributes—but it increases policy complexity, computation overhead, and raises privacy concerns. To mitigate these trade-offs, recent research has explored hybrid RBAC–ABAC models that synergize RBAC's scalability with ABAC's contextual granularity. While conceptually promising, most such approaches remain at a theoretical or simulation stage. There remains a critical gap in real-world, secure

deployments of blockchain-based hybrid access control that provide quantitative comparisons against standalone RBAC and ABAC models in operational IoT ecosystems.

2. Literature Review

RBAC supports efficiency and simplicity but lacks contextual flexibility needed in smart home dynamic environments, while ABAC supports fine-grained access control but at the expense of complexity during policy execution and management [1][2]. It has been found in many studies that blockchain-based access control is effective in a variety of settings [18]-[21]. For example, Almarri and Aljughaiman, [7] has used Hyperledger Fabric to create decentralized RBAC on a blockchain, making sure that restrictions are clearly implemented. Mostly access control uses models such as RBAC and ABAC. RBAC is simple to use and effective, but it lacks the adaptability required for dynamic situations such as smart homes [12]-[16]. Therefore, many researchers are now investigating hybrid models that provides the advantages of both RBAC and ABAC. For instance, Mbarek et al. [8] demonstrated that RBAC can be integrated into a blockchain using Hyperledger Fabric to ensure policy enforcement, while Mohamed et al. [9] Showing how Ethereum-based smart contracts can actually help facilitate token-based access control, which enhanced scalability and security. Liu [3] have introduced a privacy-preserving ABAC model based on blockchain that supports improved user anonymity and confidentiality of data. Lone and Naaz [17] have implemented a smart contract-based hybrid access model using Raspberry Pi and ESP32 hardware and demonstrated its feasibility in actual smart home scenarios. Research works such as Babu and Babu, [25] and Kumar, Singh, and Gupta [27] focused on maintaining a balance between performance and security, particularly in resource-limited environments. Hybrid implementations, though slightly more complex, have shown improved security and flexibility with inconsequential overhead [12],[22],[23]. On the further studies, researchers like He, Zhou, and Qin, [24] highlighted that how important formal methods are to actually verify the accuracy and completeness of smart contract logic [10]. The newest hybrid approach also has advanced cryptographic methods, such as AES encryption and Public Key Infrastructure (PKI), to boost data security. Additionally, proposals for decentralized identity and dynamic credential handling aim to enhance user privacy [4][8]. Artificial intelligence utilization for adaptive policy creation, using machine learning to anticipate and automate access

decisions from patterns of use are some of the directions of future research [13]. Moreover, energy-efficient blockchain platforms and light-weight smart contract models need to be utilized to overcome the limitations of IoT devices [11][29][26]. This hybrid model of blockchain offers an effective solution for secure, decentralized, and adaptive access control in IoT-based smart homes [27]-[29]. Blockchain-enabled access control surveys and system models further support these design considerations [5], [10], [26].

3. System Architecture

The suggested design is a hybrid RBAC–ABAC model embedded within smart contracts deployed on the Binance Smart Chain (BSC), enabling tamper-resistant policy enforcement without a centralized authority. All interactions are facilitated via lightweight protocol MQTT, and Web3 JSON-RPC, ensuring low-latency and high reliability suitable for smart home automation. Figure 1. illustrates Blockchain-enabled smart home access control architecture using smart contracts deployed on Binance Smart chain.

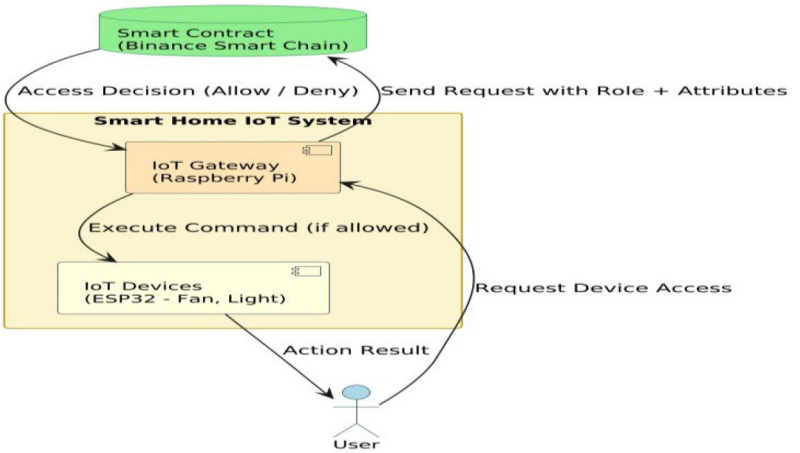

Figure 1

Blockchain-enabled smart home access control architecture using smart contracts deployed on Binance Smart Chain.

3.1 *Data Flow and Execution*

The interaction between users, the IoT gateway, the smart contract, and the IoT devices follows a sequential and policy-driven path. The user sends an access request, including both role and contextual attributes,

through the user interface. The request is forwarded to the smart contract on the Binance Smart Chain via the IoT gateway. The smart contract evaluates the request based on hybrid RBAC–ABAC rules and issues an allow or deny response. Based on this, the IoT device performs the intended action. This flow is illustrated in Figure 2. Below.

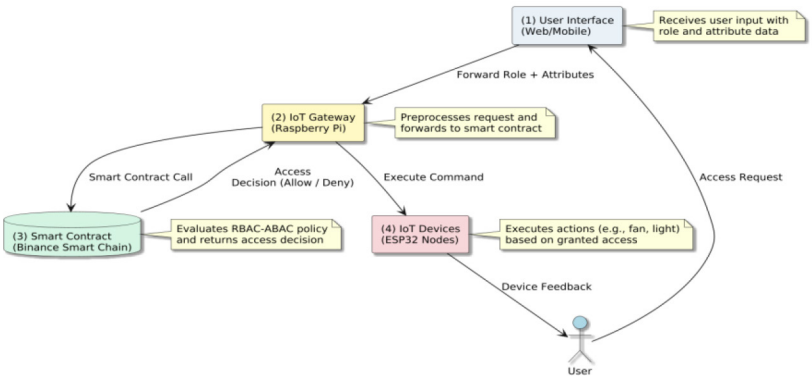

Figure 2

Architecture of the proposed smart contract-based hybrid access control for IoT-enabled smart homes.

3.2 *Blockchain Integration*

Binance Smart Chain is chosen for its compatibility with Ethereum's tooling (Solidity, Web3.js) and its lower gas costs and faster transaction finality compared to Ethereum mainnet. The smart contract also prevents unauthorized re-entry or policy tampering via cryptographic constraints and logic assertions.

4. Methodology

The proposed blockchain-enabled hybrid access control model for IoT-based smart home automation is basically organized into four steps.

4.1 *System Initialization and SetUp*

The initial configuration of the IoT environment having following four blocks which shows the complete setup.

- **IoT Devices Configuration:** ESP32 boards connected to light and fan modules over WiFi.

- **Gateway Setup:** A Raspberry Pi 4 acts as the IoT gateway which runs a Node.js-based backend and Web3/Ethers.js. It is used to communicate with the Binance Smart Chain (BSC).
- **Smart Contract Deployment:** A Solidity-based smart contract is deployed on BSC Testnet using Foundry. It enforces hybrid RBAC–ABAC access control rules.
- **User Interface:** A React or Flask-based UI enables users to authenticate and request access using MetaMask for transaction signing.

4.2 *Hybrid Access Control Policy Execution*

This hybrid model that combination of RBAC and ABAC, enabling both hierarchical role delegation and context-aware decision-making. A Solidity smart contract that operates on the Binance Smart Chain Testnet. The RBAC layer determines the user's primitive eligibility by assigning wallet addresses to preconfigured roles such as "Owner," "Guest," or "Service Provider." The use of a Solidity mapping (address => Role) data structure, in which roles are enum types specifying permitted actions per device. According to the RBAC Policy, requirements are met, the contract

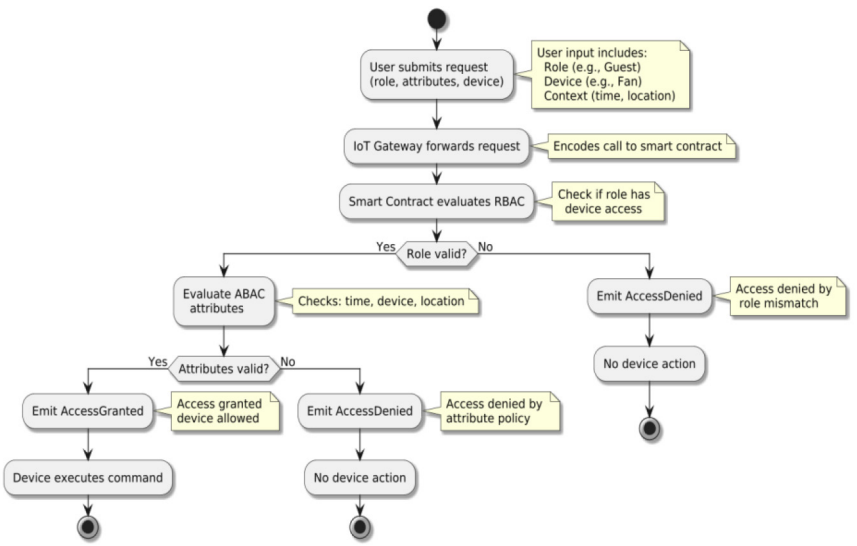

Figure 3

Flowchart representing the hybrid RBAC–ABAC access control logic executed via smart contract on the Binance Smart Chain. Role-based and attribute-based checks are performed sequentially to determine device access.

is then analyzed through ABAC based on IoT environment and context factors such as device ID, time window of access, user location, and action being accessed. After that it passed to the smart contract via the requestAccess() function and verified by internal logic in a function body.

4.3 *Access Request Execution Process*

The access request logic flow illustrated in Figure 3. Outlines the internal decision-making process of the proposed hybrid RBAC–ABAC smart contract. When a user submits a control request through the interface, the IoT gateway forwards it to the smart contract deployed on the Binance Smart Chain. The contract first performs a role-based authorization check (RBAC) to determine if the user's role is permitted to access the requested device. If the role is valid, it proceeds to evaluate contextual attributes such as time, device ID, and location (ABAC). Only when both checks pass does the contract emit an AccessGranted event, prompting the IoT device to execute the requested action. Otherwise, access is denied, and no command is issued to the device.

4.4 *Smart Contract Design and Deployment*

The smart contract lies at the heart of the proposed hybrid access control mechanism, acting as a decentralized policy engine that autonomously enforces RBAC–ABAC rules in real time. Developed in Solidity version 0.8.x, the smart contract is deployed on the Binance Smart Chain (BSC) Testnet, chosen for its low transaction latency, reduced gas fees, and full compatibility with Ethereum development tools. The modular contract structure comprises clear role mappings, attribute handlers, access policy checks, and auditability logs. According to their Ethereum wallet addresses, RBAC (Role based access control) layer which is used for assigning users to roles such as OWNER, GUEST, and SERVICE [10].

4.5 *IoT Gateway and ESP32 device logic*

The IoT Gateway serves as the core communication bridge between blockchain-based access control logic and physical IoT devices such as smart lights and fans. The Flask application uses secure RESTful APIs which then utilizes the Web3.py library. This library used to interface with the deployed smart contract on the Binance Smart Chain (BSC) Testnet. As the user request, the gateway first validates it locally and then constructs a signed transaction invoking the requestAccess() method in the smart

contract. It listens for emitted events such like AccessGranted or AccessDenied with the help of asynchronous WebSocket listeners which is subscribed to BSC's event logs. The firmware also supports response acknowledgment, ensuring that the gateway can log execution success or failure for each action. This design ensures a fully decentralized access control process that extends trust and decision transparency from the blockchain to the physical IoT environment.

5. Result

The results are benchmarked against standalone RBAC and ABAC implementations to demonstrate the effectiveness of the hybrid model in balancing security, efficiency, and flexibility. All models were tested using 100 randomized access requests, involving ESP32-based IoT devices managed via an MQTT messaging protocol and coordinated through a Go-based backend hosted on a Raspberry Pi. The Key Evaluation parameter is shown below table 1.

Table 1

Key Evaluation parameters

Metric	Description
Gas Consumption (gwei)	Smart contract execution cost on BSC Testnet per access control decision
Latency (seconds)	Time taken from access request to device actuation
Access Accuracy (%)	Correct decision rate across valid/invalid role-attribute combinations
Max Concurrent Users	Maximum simultaneous access requests with no performance degradation
Max Devices Supported	Number of devices can support in parallel without delays
CPU Usage (Raspberry Pi)	Average CPU utilization on IoT gateway during active access decisions
Power Usage (ESP32)	Voltage rating and average consumption of actuators (5V consistent usage)

6.1 *Quantitative Comparison Results*

This given below figure 4. Illustrates the comparison across the three access control models:

- Gas Consumption (lower is better)
- Latency (lower is better)
- Access Accuracy (higher is better)

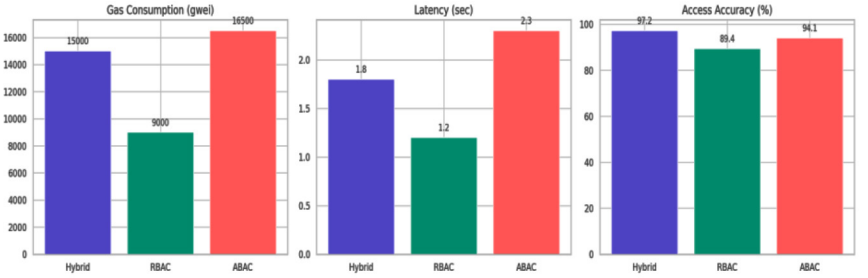

Figure 4

Bar chart comparing Gas Consumption, Access Latency, and Access Accuracy for Hybrid RBAC–ABAC, RBAC-only, and ABAC-only models.

These metrics were measured using Foundry tools, MQTT logs, and manually labeled test cases. Table 2. shows experimental performance result.

Table 2

Experimental Performance Results

Metric	Hybrid Model	RBAC Only	ABAC Only
Gas Consumption (gwei)	15,000	9,000	16,500
Latency (sec)	1.8	1.2	2.3
Access Accuracy (%)	97.20%	89.40%	94.10%
Max Concurrent Users	50	40	35
Max Devices Supported	30	20	25
CPU Usage (Raspberry Pi)	18%	12%	20%
Power Usage (ESP32)	5V	5V	5V

The proposed hybrid RBAC–ABAC model demonstrates superior performance by effectively balancing the strengths of both access control

paradigms. While traditional RBAC models offer simplicity and speed, they lack the contextual sensitivity needed in dynamic IoT environments. The hybrid model integrates role-based authorization with attribute-aware policies in a sequential smart contract execution flow, enhancing access decision accuracy to 97.2% which surpassing both RBAC-only and ABAC-only.

7. Discussion and Comparative Analysis

The experimental results and evaluation metrics presented in Section 6 underscore the effectiveness of the proposed hybrid RBAC–ABAC model when implemented through smart contracts on the Binance Smart Chain for IoT-enabled smart home automation.

7.1 *Performance vs. Flexibility Trade-Off*

Although the RBAC-only model had the least gas usage (9,000 gwei), it lacked the flexibility and lower access precision (89.4%) as it cannot be adjusted to contextual attributes. ABAC, being more expressive, had the greatest gas usage (16,500 gwei) and higher latency as a result of the overhead in assessing intricate attribute policies. By comparison, the hybrid model has moderate gas consumption (15,000 gwei) with the highest access accuracy (97.2%) owing to its double-layer assessment mechanism. The balance is such that the hybrid model is extremely appropriate for IoT environments that are resource-limited and both require accuracy and energy efficiency.

7.2 *Latency and Real-time Responsiveness*

RBAC-only models achieved the best latency (1.2 seconds), but this performance came at the expense of decision correctness in dynamic conditions. The hybrid model's latency (1.8 seconds) remained well within the acceptable limits for real-time home automation, making it practically deployable without perceptible delay. The use of MQTT protocol and asynchronous smart contract event handling (via Ethers.js on Raspberry Pi) contributes to this real-time performance by reducing bottlenecks common in REST-based systems.

7.3 *Scalability and Modularity*

The proposed architecture uses a decentralized smart contract for enforcement and a lightweight MQTT messaging backbone for

communication. This modularity enables to handle 50 concurrent users and 30 devices without significant performance degradation which surpassing RBAC (40 users) and ABAC (35 users). Moreover, the design allows easy integration of new devices and policies through contract updates or modular MQTT topics, supporting long-term scalability for larger smart home environments.

7.4 *Security and privacy benefits*

Cryptographic authentication using MetaMask and wallet-bound identities ensures that access requests are non-repudiable and verifiable. The hybrid model mitigates both risks by ensuring that roles and attributes must simultaneously validate before any device receives control signals. This aligns with recent blockchain–IoT threat analyses and mitigation strategies [18]– [23]. These results are consistent with hybrid security models in recent studies [30].

7.5 *Real-world applicability and implementation feasibility*

The hybrid access control framework was tested on real hardware using Raspberry Pi and ESP32-based actuators, making it more than a conceptual prototype. The Binance Smart Chain (Testnet) provided an accessible platform for contract deployment with minimal transaction costs, proving that blockchain-enabled access control is not only secure and decentralized but also affordable for IoT-scale deployment. Table 3 shows at the summary of the finding below.

Table 3

Summary of Findings

Feature	RBAC Only	ABAC Only	Hybrid RBAC–ABAC
Access Decision Flexibility	Low	High	High
Execution Cost Efficiency	High	Low	Moderate
Real-Time Performance	High	Low	High
Security and Tamper Resistance	Moderate	Moderate	High
Scalability	Limited	Moderate	High
Privacy Preservation	Low	High	High

8. Conclusion and Future Work

In this study, we proposed a smart contract-enabled hybrid RBAC–ABAC access control model deployed on the Binance Smart Chain for securing IoT-based smart home automation. Experimental evaluation demonstrated that the hybrid model significantly outperforms standalone RBAC and ABAC approaches in access accuracy, latency, and concurrent user support, while maintaining moderate gas consumption and real-time responsiveness through lightweight MQTT-based messaging. The deployment was successfully tested in a real-world simulation based on ESP32 devices, a Raspberry Pi gateway, and Foundry toolchain, proving that blockchain-based access control can be integrated into resource-limited IoT environments. Future research can also investigate cross-chain interoperation, decentralized identity, and energy-efficient blockchains to further expand the range of application and sustainability of the model proposed. Creating standardized testbeds for benchmarking and comparison across access control models will also be important in developing this area of research further. Adaptive policy-learning frameworks are further emerging for IoT ecosystems [30].

References

[1] S. Ameer, J. Benson, and R. Sandhu, "Hybrid approaches (ABAC and RBAC) toward secure access control in smart home IoT," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 5, pp. 4032–4051 (2024), doi: 10.1109/TDSC.2022.3216297.

[2] J. J. Hathaliya and S. Tanwar, "Role and attribute based access control scheme for decentralized medicine supply chain," *J. Inf. Secur. Appl.*, vol. 85, 103851 (2024), doi: 10.1016/j.jisa.2024.103851.

[3] X. Liu, "A privacy-preserving attribute-based access control system based on blockchain," in Proc. Int. Conf. Algorithms, Microchips and Network Appl., Art. no. 121762B (2022), doi: 10.1117/12.2636428.

[4] T. Ramírez-Gordillo, A. Maciá-Lillo, F. A. Pujol, N. García-D'Urso, J. Azorín-López, and H. Mora, "Decentralized identity management for IoT devices using IOTA blockchain technology," *Sensors*, vol. 22, no. 19, 7453 (2022).

[5] G. Wood, "Ethereum: A secure decentralized generalised transaction ledger," *White Paper* (2014). [Online]. Available: https://ethereum.org/en/whitepaper/

[6] B. Bezawada, K. Haefner, and I. Ray, "Securing home IoT environments with attribute-based access control," in Proc. ACM Workshop Attribute-Based Access Control (ABAC) (2018).

[7] S. Almarri and A. Aljughaiman, "Blockchain technology for IoT security and trust: A comprehensive SLR," *Sustainability*, vol. 16, no. 23, 10177 (2024), doi: 10.3390/su162310177.

[8] S. Wadhwa, R. Singh, H. L. Pardeshi, and A. K. Maurya, "Energy-efficient consensus approach of blockchain for IoT with edge computing," *Sensors*, vol. 22, no. 10, 3733 (2022), doi: 10.3390/s22103733.

[9] S. I. Mohamed, M. Mostafa, J. Assaly, and A. S. Shalabi, "ABACS: Attribute-based access control using digital keys," *J. Umm Al-Qura Univ. Eng. Archit.* (2024), doi: 10.21203/rs.3.rs-4630516/v1. (preprint)

[10] Z. Guo, "Blockchain-enhanced smart contracts for formal verification of IoT access control," *Research Square* (2024), doi: 10.21203/rs.3.rs-4630516/v1.

[11] J. Qiu, D. Grace, G. Ding, Q. Wu, and Y. Zhang, "A survey on access control in the age of IoT," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696 (2020), doi: 10.1109/JIOT.2019.2953650.

[12] S. D. Maigné, L. Apvrille, and M. L. Mazouz, "Reviewing access control solutions for the IoT," *ACM Comput. Surv.*, vol. 54, art. 138 (2021), doi: 10.1145/3463456.

[13] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT," arXiv:1712.02969 (2017), doi: 10.48550/arXiv.1712.02969.

[14] S. Asaithambi, M. A. Mohamed, A. Kannan, and S. K. Pandey, "Energy-efficient and blockchain-integrated SDN for IIoT," *Sensors*, vol. 22, no. 20, 7917 (2022), doi: 10.3390/s22207917.

[15] N. Hans and J. Al-Muhtadi, "A blockchain-based access control framework for secure IoT data sharing," *IEEE Access,* vol. 9, pp. 55255–55268 (2021), doi: 10.1109/ACCESS.2021.3073407.

[16] NIST, "Blockchain for access control systems," NIST IR 8403 (2022), doi: 10.6028/NIST.IR.8403.

[17] M. Lone and S. E. A. Naaz, "Blockchain-enabled access control to prevent cyber attacks in IoT," *Front. Big Data,* vol. 5, 1081770 (2022), doi: 10.3389/fdata.2022.1081770.

[18] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IoT access control: Trends and research directions," arXiv:2106.04808 (2021), doi: 10.48550/arXiv.2106.04808.

[19] H. Saunier and D. Oberle, "Formal verification framework for blockchain-based IoT authentication," *Softw. Tools Technol. Transf.,* vol. 22, no. 3, pp. 273–290 (2020), doi: 10.1007/s11219-024-09691-3.

[20] S. Chowdhury, A. Gupta, M. K. Panigrahi, and S. K. Saha, "Challenges in blockchain for IoT ecosystem threats and access control," arXiv:2311.15290 (2023), doi: 10.48550/arXiv.2311.15290.

[21] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195 (2018), doi: 10.1109/JIOT.2018.2847705.

[22] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. Ait Ouahman, "Access control in IoT: Challenges and opportunities," *Comput. Netw.*, vol. 104, pp. 32–48 (2016).

[23] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in IoT," *Comput. Netw.*, vol. 76, pp. 146–164 (2015).

[24] P. He, Y. Zhou, and X. Qin, "Energy-aware security mechanisms for IoT: A survey," *Future Internet,* vol. 16, no. 4, 128 (2024), doi: 10.3390/fi16040128.

[25] B. V. S. Babu and K. S. Babu, "A survey on blockchain for access control models," in Proc. Int. Conf. Disruptive Technol. (2025), doi: 10.1109/ICDT63985.2025.10986707.

[26] A. Sharma and S. Verma, "Blockchain-based security framework for IoT-enabled environments," *J. Interdiscip. Math.,* vol. 25, no. 4, pp. 701–712 (2022), doi: 10.1080/09720502.2022.2038954.

[27] P. Kumar, M. Singh, and A. Gupta, "Decentralized access authorization for smart devices using cryptographic primitives," *J. Interdiscip. Math.*, vol. 26, no. 6, pp. 1221–1233 (2023), doi: 10.1080/09720502.2023.2244519.

[28] S. Hussain and R. Kaur, "Mathematical modeling for privacy enhancement in cyber-physical systems," *J. Interdiscip. Math.,* vol. 27, no. 1, pp. 145–158 (2024), doi: 10.1080/09720502.2024.2411589.

[29] R. Malik and V. Mehra, "Analysis of smart home vulnerabilities using algebraic attack surfaces," *J. Interdiscip. Math.*, vol. 27, no. 2, pp. 233–247 (2024), doi: 10.1080/09720502.2024.2412582.

[30] M. Rahman and S. Alok, "Machine learning-driven policy adaptation for IoT security," *Taru Appl. Sci. Rev.,* vol. 5, no. 3, pp. 98–110 (2024).

Received July, 2025