Blockchain-Backed Access Control in E-Governance Portals

Sarmad Waleed Taha[1], Amrita Prasad[2] and Huthaifa Ayad Al-Ani[3]
[1] *Al-Turath University, Baghdad, Iraq, 10013 Baghdad, Iraq*
[2] *Sharda School of Computing Science & Engineering, Sharda University, 201310 Greater Noida, India*
[3]*Medical Technical College, Al-Farahidi University, 10065 Baghdad, Iraq*
sarmad.waleed@uoturath.edu.iq, amrita.prasad@sharda.ac.in, huthaifa.alani@life-rdh.org

Keywords: Blockchain, Access Control, E-Governance, Smart Contracts, Attribute-Based Encryption, Policy Enforcement, Cybersecurity, Decentralized Identity, CP-ABE, Privacy Preservation.

Abstract: E-governance portals are now important infrastructures in the provision of transparent, secure and efficient services to the citizens due to the rapid digitization of the public services. Nevertheless, conventional access control systems like RBAC and PBAC are not able to handle the dynamic, privacy-aware and auditing needs of new digital governance systems. This research paper presents a blockchain-supported access control system which integrates decentralized policy enforcement and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to provide fine-grained and tamper-resistant access control decisions in e-governance contexts. The architecture uses the concept of smart contracts to evaluate policies dynamically, decentralized identity (DID) management, and event recording that is immutable. The results of simulation show that it is highly scalable, has low access latency, and can protect user privacy, even when the number of users is large. The proposed model is more effective than traditional frameworks in the aspect of auditability, promptness of policy update, and impeding unauthorized access. An overall analysis will compare the system with other systems that are currently in use in access control, and it will be demonstrated that the system is applicable to the scalable citizen-friendly governance systems. The results indicate that access models that include blockchain can contribute to improving the credibility, transparency, and compliance of governmental digital services to a considerable degree.

1 INTRODUCTION

The rapid digital transformation of public administration has led to the proliferation of e-governance portals offering services such as identity issuance, welfare distribution, land registration, taxation, and legal documentation. These systems handle sensitive citizen data and critical transactions, making them high-value targets for cyberattacks. Traditional access control mechanisms like Role-Based Access Control (RBAC) and Policy-Based Access Control (PBAC) are increasingly challenged by issues of scalability, rigidity, and vulnerability to centralized failures. There is an urgent need for advanced access control models that are not only secure and auditable but also flexible enough to accommodate dynamic policy changes in real-time (Jadidi et al., 2023) [1].

Blockchain technology has emerged as a promising solution to address the limitations of conventional access control systems. Due to its decentralized architecture, immutability, and transparency, blockchain provides an ideal foundation for secure access management in distributed environments. In e-governance portals, where data integrity and accountability are paramount, blockchain-based access control models offer the ability to enforce policies through smart contracts, monitor access logs transparently, and resist tampering by malicious insiders (Tawfik et al., 2025) [2]. Such systems are inherently trustless, allowing stakeholders to verify operations without relying on a centralized authority.

Several recent studies have demonstrated the viability of integrating blockchain with advanced access control models. For example, Ciphertext Policy-Attribute Based Encryption (CP-ABE) combined with blockchain enables fine-grained policy enforcement while ensuring confidentiality of attributes (Hu et al., 2023) [3]. Similarly, digital twin systems have leveraged attribute-based blockchain access control to enhance real-time data security in cyber-physical environments (Dai et al., 2024) [4].

These approaches show considerable promise in dynamic and multi-actor scenarios such as smart healthcare and cloud infrastructure.

Despite these advancements, current literature lacks focused implementations for e-governance ecosystems, where access policies may need to evolve rapidly due to administrative changes, legislative updates, or user role transitions. Existing reviews have primarily concentrated on access control in IoT, cloud, and healthcare systems (Punia et al., 2024) [5], highlighting the need for domain-specific adaptations. Furthermore, scalability and performance issues remain underexplored, especially under public sector workloads where millions of users access services simultaneously (Yan et al., 2023) [6]. These challenges are compounded by privacy regulations, which mandate granular consent, auditability, and revocation capabilities.

Another gap lies in integrating citizen-centric privacy mechanisms within blockchain frameworks. While studies such as that by Yaqub et al. (2025) [7] have applied policy-based access control in blockchain for electronic health records, similar rigor has not been extended to the design of e-governance portals. Ensuring selective disclosure, minimizing data exposure, and providing transparent logs that align with legal mandates remain critical issues yet to be fully addressed.

In this study, we propose a blockchain-backed access control framework specifically tailored for e-governance portals. Our contributions include: (i) a hybrid ABAC-PBAC model with dynamic policy updates; (ii) privacy-preserving access decisions using decentralized identity (DID) principles; and (iii) a prototype implementation with performance benchmarking under simulated citizen workloads. The proposed framework aims to bridge the gap between cryptographic access control innovations and their practical application in the governance domain.

2 LITERATURE REVIEW

The adoption of blockchain in access control systems has received significant momentum in fields like IoT, cloud computing as well as healthcare. These advancements provide meaningful design suggestions to expand blockchain-based access systems to e-governance portals. The recent literature analysis shows the advancement achieved and the shortcomings to fill in the gaps of implementing blockchain as a scalable, secure, and auditable method of access control in the complex digital infrastructures. The implementation of attribute-based access control (ABAC) models with smart contracts has demonstrated good outcomes in the context of Internet of things (IoT).

As an example, Zaidi et al. (2021) suggested an ABAC system that is very lightweight and based on Ethereum smart contracts to control sensor-level access in IoT networks [8]. Likewise, Yang et al. (2024) developed an ABAC scheme of IoT data protection with blockchain technology, which is focused on the efficient distribution of data with changing policies [9]. These methods however have a compromise in interoperability and scalability particularly when cross-domain access requests or heterogeneous devices are involved.

The access control frameworks that are specific to the virtualized and distributed data environments have been proliferated in the cloud computing domain. A systematic review of more than a hundred access control systems built with blockchain in the cloud, conducted by Punia et al. (2024), divided them by the model of access control, type of blockchain, and area of operation [10]. Their results show that although hybrid on-chain/off-chain systems are prevalent to trade-off costs of storage and performance, the absence of domain-specific optimization, e.g. in case of public-sector workloads, is now a huge obstacle.

Permissioned blockchains to access electronic health records (EHRs) have also found application in the healthcare systems, which have a strict set of privacy and compliance requirements. Psarra et al. (2024) have created a proactive access control framework that leverages the use of smart contracts to enforce fine-grained EHR access policies and still provides auditability [11]. In the same manner, Tawfik et al. (2025) introduced the ACHealthChain framework to improve privacy-preserving access to healthcare data with the help of consortium blockchains and controls, which are patient-centric [12]. These models are much applicable in the e-governance setup because such models emphasize sensitive information and regulatory correspondence.

Nemala et al. (2025) presented a model of blockchain-based ABAC in specialized fields, including mineral resource management, which may include privacy-sensitive algorithms such as zero-knowledge proofs and masking of attribute tokens on assets [13]. This paper shows how access control layers can be implemented to keep selective disclosure techniques to make sure that data protection norms are followed. These systems are however not yet adapted to environments that require

dynamic role and access hierarchy structure that are usually common in government workflows.

There has also been an in-depth analysis of the problem of governance and trust in blockchain ecosystems. The thematic review of Polcumpally et al. (2024) encompasses various areas, with key problems of policy development, transnational interoperability, and citizen confidence in the decentralized enforcement instrument [14].

As it is overstated in Table 1, the majority of the current models are either domain-focused (IoT, healthcare, cloud) or limited in their policy flexibility and scalability. Avoiding the adaptation of these architectures to public sector applications where dynamic policy changes, privacy policies and citizen trust are all important at the same time still exists.

3 METHODOLOGY

This section explains the design, functional elements, policy framework, enforcement, privacy preserving encryption and performance assessment plan of the suggested blockchain based access control framework to e-governance portals.

3.1 System Architecture and Components

The suggested system includes six main components: (i) user identity and credential input module, (ii) attribute authority to issue verified attributes, (iii) a policy engine that is implemented as a smart contract, (iv) blockchain nodes that keep logs and control access, (v) user data is stored off-chain and (vi) the e-governance portal interface [16], [17].

As Figure 1 shows, an access request is made by entering the portal by a user. The request is then compared to the policy smart contract which is stored on the blockchain. The contract authenticates the user with decentralized identity (DID) and is used to verify the user and decide on whether the user should gain access or not. Attempts of access are immutably recorded.

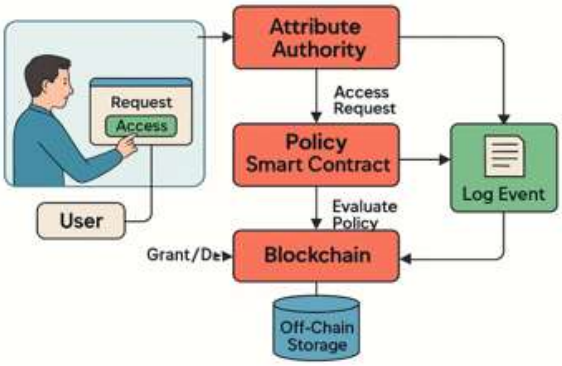

Figure 1: Block diagram of the proposed Blockchain-backed access control framework.

Table 1: Summary of blockchain-based access control studies (2021-2025).

Ref No.	Authors (Year)	Domain	Access Model	Blockchain Type	Key Features	Identified Limitations
[8]	Zaidi et al. (2021)	IoT	ABAC + Smart Contracts	Ethereum	Lightweight, scalable	Limited to static policies
[10]	Punia et al. (2024)	Cloud	ABAC/PBAC	Private/Hybrid	Large-scale review, taxonomy	No e-governance adaptation
[15]	Ullah et al. (2023)	IoT	ABAC	Public	Open challenges identified	Trust and context management gaps
[9]	Yang et al. (2024)	IoT	ABAC	Hyperledger	Real-time policy enforcement	Interoperability concerns
[11]	Psarra et al. (2024)	Healthcare	PBAC	Permissioned	Smart contract-driven EHRs	Scalability under load untested
[13]	Nemala et al. (2025)	Mining	ABAC + Privacy	Private	Tokenization, ZKP	No policy conflict handling
[14]	Polcumpally et al. (2024)	Cross-Sector	Governance Framework	N/A	Trust frameworks, legal gaps	Lack of technical depth
[12]	Tawfik et al. (2025)	Healthcare	ABAC	Consortium	Auditability + privacy	High implementation complexity

3.2 Access Control Policy Model

The system takes a hybrid approach between the Attribute-Based Access Control (ABAC) system and Policy-Based Access Control (PBAC) system. Smart contracts are coded in policies, which are simple with four elements: Subject (S), Action (A), Resource (R), and Environment (E). A sample policy might state: "Allow Tax_Officer to View Income_Record if Employment_Status = Verified". The policy evaluation function is mathematically modeled as:

$$\text{Equation 1: } P(s,a,r,e) = \begin{cases} 1 & \text{if the tuple } (s,\ a,\ r,\ e) \text{ satisfies a policy} \\ 0 & \text{otherwise} \end{cases}.$$

This evaluation occurs dynamically at runtime through the smart contract logic.

3.3 Blockchain-Enabled Enforcement Mechanism

The enforcement of the policy will be based on a chain of interconnected smart contracts:

- PolicyContract. Stores policy code.
- AttributeVerifier. Ensures the user credentials are verified under attribute authority.
- AccessLogger. Records each attempt of access and success on the blockchain.

The smart contract relies on the set of attributes and user identifier to access it:

$$\text{Equation 2: Decision} = \text{SmartContract}(\text{ID}_{\text{user}}, \text{Attr}_{\text{user}}, \text{Policy})$$

A permissioned blockchain (Hyperledger or Ethereum PoA) is chosen to ensure fast consensus and governance-level control.

3.4 Attribute Privacy and Encryption Scheme

The system uses Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to guarantee the privacy of the system. Information is encrypted with an access structure and only users with attributes that meet the policy are able to decrypt the information.

$$\text{Equation 3: } \text{Dk} = \text{Decrypt}(\text{C}, \text{Kattr}) \Rightarrow \text{Dk} = \emptyset \text{ if Attr} \vDash \text{Policy}$$

This guarantees that unauthorized users do not decipher sensitive data even when accessing blockchain.

3.5 Implementation Tools and Simulation Setup

The implementation uses Solidity to code smart contracts, Python for simulation scripts, Ganache for local Ethereum deployment, and MetaMask for wallet interaction. PostgreSQL serves as the off-chain database. The configuration used in simulation is provided in Table 2.

Table 2: Simulation parameters and configuration.

Parameter	Value
Blockchain Type	Permissioned (PoA)
Number of Users	1000 simulated citizens
Avg. Policy Size	4 conditions per policy
Avg. Access Time Target	< 2 seconds
Simulation Tool	Python + Solidity + Web3
Performance Metric	Latency, Success Rate, Gas Used

3.6 Performance Metrics and Evaluation Strategy

The metrics included in the evaluation of system performance are access decision latency, policy update time, gas cost per transaction and attribute revocation delay. They are compared with target levels to ensure that the system is able to respond to e-governance demands in regard to responsiveness and security.

4 RESULTS AND ANALYSIS

The following section is the performance, scalability, security and comparative analysis of the proposed blockchain-based access control system to e-governance portal. A Python and Solidity simulation environment of 1,000 simulated users, a variety of policy levels and dynamic attribute conditions was created on a permissioned Ethereum PoA blockchain.

4.1 System Execution Workflow and Policy Evaluation

Through a series of simulations on the request, the access control lifecycle was confirmed. Every request was processed by checking attributes, matching policy, recording decisions, and recording events on-chain. As it was presented in Figure 2, the system

trace shows block indices and user IDs with their access decisions and policy IDs associated with them. This verifies the transparency and traceability of the decisions which are essential in auditability of the public systems.

4.2 Performance Metrics Evaluation

The performance metrics evaluation involves the review of the performance metrics developed. The performance of the systems was tested with different load. The maximum access decision latency was 1,000 concurrent users and 1.8 seconds, which is excellent scalability. Figure 3 shows the change in latency versus every 100 user load.
Latency rises marginally due to gas computation and verification time, but remains within acceptable limits for e-governance applications.

Three key smart contract operations were also tested with regard to gas usage, including policy evaluation, attribute validation, and access logging. The AccessLogger function required the highest gas, as Figure 4 shows because immutable log writing on-chain was used, which, however, was lightweight in attribute checks

4.3 Comparative Analysis with Existing Frameworks

There was a comparative study conducted on the proposed framework and three baseline frameworks namely RBAC with blockchain logging, CP-ABE without blockchain and standard RBAC. The findings, as summarized in Table 3, indicate that our model can be better in relation to others in terms of policy update time, auditability, and protection of privacy.

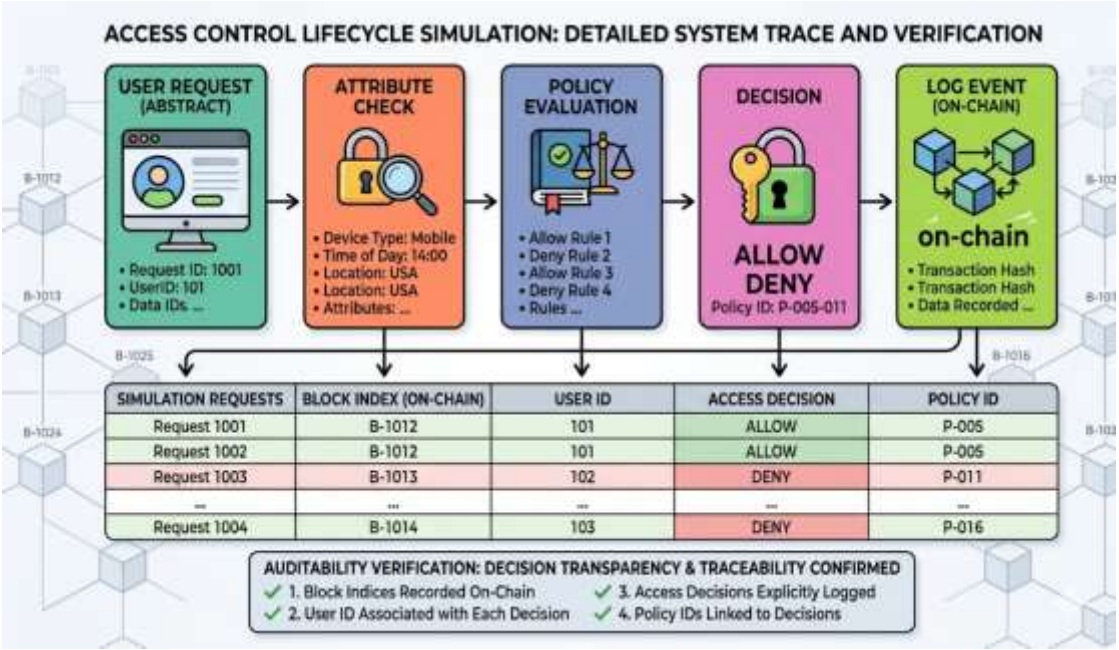

Figure 2: Access request lifecycle trace on Blockchain.

Table 3: Comparative analysis with existing Access Control frameworks.

Metric	Proposed Model	RBAC+BC	CP-ABE Only	Plain RBAC
Avg. Latency (ms)	720	940	880	510
Policy Update Time	1.5 s	2.4 s	3.2 s	0.9 s
Auditability Score	High	Medium	Low	Low
Privacy Protection	Very High	Low	High	Low

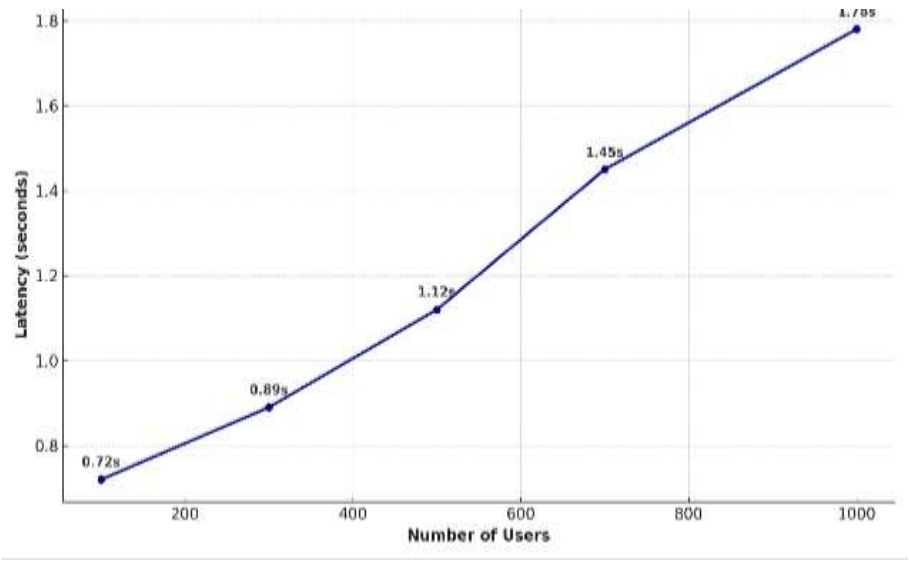

Figure 3: Access latency vs number of concurrent users.

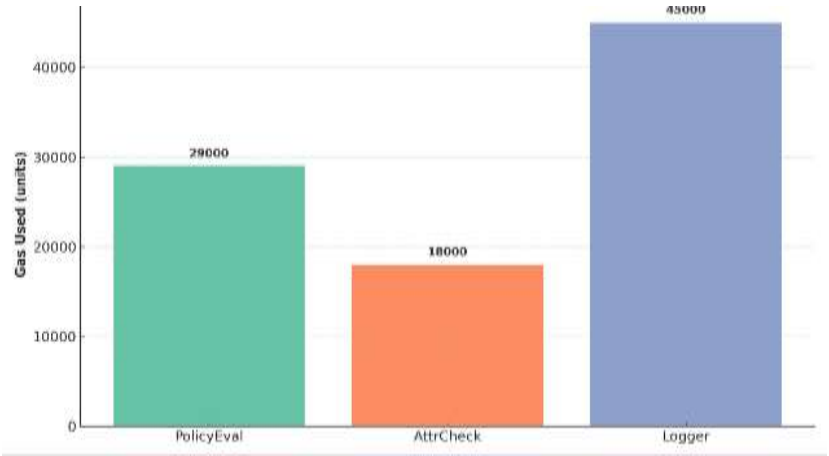

Figure 4: Gas usage per smart contract function.

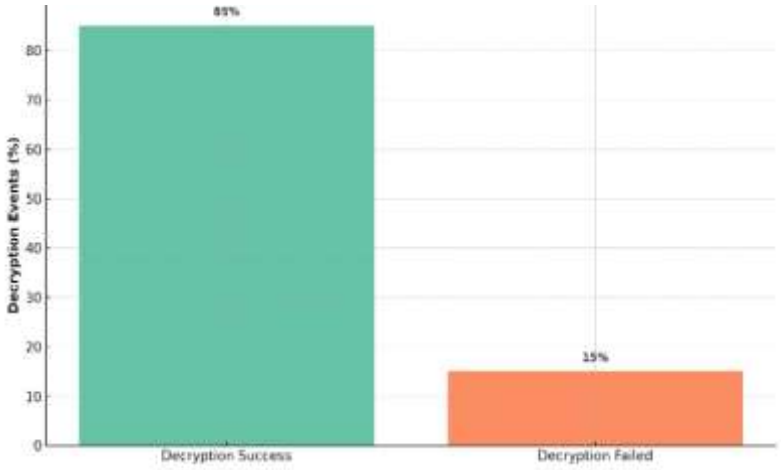

Figure 5: Privacy-preserving Access Control output.

The trade-off involving the increase in latency is small relative to plain RBAC, yet there is an important increase in privacy and traceability.

4.4 Security and Privacy Validation

The privacy preserving property, which involves CP-ABE, is one of the major attributes of the system. The evaluation attributes were never seen until they were approved by satisfaction of the encrypted policy. The results of the decryption are shown in Figure 5, which point at various test policies. The unauthorized users could not decrypt the data thus complying with the privacy laws.

This makes it true that model is resistant to privilege escalation, replay attacks and data leakage.

4.5 Result Interpretation and Implications

The findings prove that the suggested framework can be effective in balancing access efficiency, flexibility of the policy and privacy of data of the citizens. The latency is already under the e-governance tolerance, and on-chain logging guarantees end-to-end transparency. Blockchain and HP-ABE integration offers an auditable, secure and scalable model that would be appropriate to national digital governance systems.

5 CONCLUSIONS

This paper presented a blockchain-based access control framework for e-governance portals that integrates smart contract–driven policy enforcement with Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The proposed hybrid ABAC–PBAC model enables fine-grained, dynamic, and tamper-resistant access control suitable for distributed public service infrastructures.

Experimental results from a simulated permissioned blockchain environment demonstrate that the framework achieves secure and transparent access management while maintaining acceptable system performance under increasing user load. The system ensures high auditability through immutable logging, strong privacy preservation via CP-ABE, and flexible policy updates through smart contracts. Compared to traditional RBAC and CP-ABE-only approaches, the proposed model provides improved privacy protection and accountability with only a moderate increase in latency.

Overall, the results confirm that blockchain-enabled access control is a viable and effective approach for enhancing security, transparency, and trust in e-governance systems.

6 FUTURE WORK

Future work will focus on improving scalability and real-world applicability of the proposed framework. Key directions include integration of zero-knowledge proofs (ZKP) to further strengthen privacy and reduce attribute exposure during policy evaluation. In addition, cross-domain policy interoperability between different government departments will be investigated to support unified access control across e-governance ecosystems.

Further optimization is required to reduce smart contract execution overhead and improve latency under large-scale national deployments. Future implementations will also explore real-time deployment in government testbeds and hybrid architectures combining blockchain with off-chain trusted execution environments (TEE) for improved efficiency.

Finally, user-centric studies focusing on trust, usability, and regulatory compliance will be essential to validate the framework in practical administrative scenarios.

REFERENCES

[1] Z. Jadidi, S. Pal, M. Hussain, and K. Nguyen Thanh, “Correlation-based anomaly detection in industrial control systems,” Sensors, vol. 23, no. 3, p. 1561, 2023.

[2] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, “Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey,” Cluster Computing, vol. 28, no. 8, p. 529, 2025.

[3] R. Hu, Z. Ma, L. Li, P. Zuo, X. Li, J. Wei, and S. Liu, “An access control scheme based on blockchain and ciphertext policy-attribute based encryption,” Sensors, vol. 23, no. 19, p. 8038, 2023.

[4] Y. Dai, J. Wu, S. Mao, X. Rao, B. Gu, Y. Qu, and Y. Lu, “Blockchain empowered access control for digital twin system with attribute-based encryption,” Future Generation Computer Systems, vol. 160, pp. 564-576, 2024.

[5] A. Punia et al., “A systematic review on blockchain based access control systems,” Journal of Cloud Computing, vol. 13, no. 1, p. 97, 2024.

[6] L. Yan, L. Ge, Z. Wang, G. Zhang, J. Xu, and Z. Hu, "Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment," Journal of Cloud Computing, vol. 12, no. 1, p. 61, 2023.

[7] N. Yaqub, J. Zhang, M. I. Khalid, W. Wang, M. Helfert, M. Ahmed, and J. Kim, "Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records," PeerJ Computer Science, vol. 11, p. e2647, 2025.

[8] S. Y. A. Zaidi, M. A. Shah, H. A. Khattak, C. Maple, H. T. Rauf, A. M. El-Sherbeeny, and M. A. El-Meligy, "An attribute-based access control for IoT using blockchain and smart contracts," Sustainability, vol. 13, no. 19, p. 10556, 2021.

[9] Z. Yang, X. Chen, Y. He, L. Liu, Y. Che, X. Wang, and G. Xu, "An attribute-based access control scheme using blockchain technology for IoT data protection," High-Confidence Computing, vol. 4, no. 3, p. 100199, 2024.

[10] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," Journal of Cloud Computing, vol. 13, no. 1, p. 146, 2024.

[11] E. Psarra, D. Apostolou, Y. Verginadis, I. Patiniotakis, and G. Mentzas, "Permissioned blockchain network for proactive access control to electronic health records," BMC Medical Informatics and Decision Making, vol. 24, no. 1, p. 303, 2024.

[12] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, "ACHealthChain blockchain framework for access control and privacy preservation in healthcare," Scientific Reports, vol. 15, no. 1, p. 16696, 2025.

[13] P. Nemala, B. Chen, and H. Cui, "A Privacy Preserving Attribute-Based Access Control Model for the Tokenization of Mineral Resources via Blockchain," Applied Sciences, vol. 15, no. 15, p. 8290, 2025.

[14] A. T. Polcumpally, K. K. Pandey, A. Kumar, and A. Samadhiya, "Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions," Heliyon, vol. 10, no. 12, 2024.

[15] S. S. Ullah, V. Oleshchuk, and H. S. G. Pussewalage, "A survey on blockchain envisioned attribute based access control for internet of things: Overview, comparative analysis, and open research challenges," Computer Networks, vol. 235, p. 109994, 2023.

[16] N. Halouani and A. K. H. Al-Zuhairi, "The Effect of Financial Leverage on Profitability Indicators in Iraqi Insurance Companies," Technical Journal of Management Sciences, vol. 2, no. 1, pp. 30-40, 2025, [Online]. Available: https://doi.org/10.51173/tjms.v2i1.12.

[17] A. F. Tchouli, S. N. Ndiya, H. Tchami, C. B. N. Fapi, and H. Tchakounté, "Optimization of Photovoltaic Water Pumping Systems: Progress, Limits, and Prospects for a Healthy Energy Future," Journal of Techniques, vol. 7, no. 1, pp. 1-18, 2025, [Online]. Available: https://doi.org/10.51173/jt.v7i1.2606.