International Innovative Research Journal of Engineering and Technology
Vol. 11, Issue. 2, Dec 2025, pp. 26~37
ISSN: 2456-1983, ORCID: 10.32595/iirjet.org/v11i2.2025.235

A Review of Blockchain-Driven Access Control Frameworks for Secure Smart Contracts in Cloud Environments

Marwa Ali Hamdan AL-Jabri[1], Nafisa Abul Ghafoor Othman AL-Ansari[2]
[1]Department of Information Technology, University of Technology and Applied Sciences, Shinas, Oman
[2]Department of Information Technology, University of Technology and Applied Sciences, Shinas, Oman

Article Info

Article History:

Received Oct 18 2025
Revised Nov 16, 2025
Accepted Dec 12, 2025

Keywords:

Blockchain
Access control
Smart contracts
Decentralized identity
Attribute-based access control
Cloud computing security
Privacy-preserving systems

ABSTRACT

Access control is an important part of cybersecurity in distributed systems since conventional centralized mechanisms are not always sufficient. Due to blockchain, individuals have begun to employ decentralized access control models as they are capable of enhancing transparency, auditing and defending against fraud. At the reason of this report, we survey various blockchain-based access control systems, paying special attention to their architectures, confirmation mechanisms, identity models and policy enforcement mechanisms. We categorize the current literature into various groups based on their platforms (e.g. Ethereum, Hyperledger, Fabric), control mechanisms (e.g. RBAC, ABAC and capability-based) and whether they introduce additional privacy-tools such as zero-knowledge proofs and decentralized identifiers. The paper analyzes and describes the key gaps in current frameworks in terms of scalability, interoperability and computing expenses. Then, the shortcomings of the current research are pointed out so that they could guide future efforts in the field of blockchain-based access control systems.

Corresponding Author:

Marwa Ali Hamdan AL-Jabri,
Department of Information Technology,
University of Technology and Applied Sciences, Shinas, Oman.

1. INTRODUCTION

As digital systems tend to be decentralized, ensuring the security of access control has become of high importance to cloud systems [1], IoT systems and distributed applications. RBAC, DAC and MAC are models that are typically unable to manage the demands of dynamic cloud environments since they were designed in predetermined, single user scenarios. Since blockchains have a reliance on a primary organization, this makes one significant item that can go down, in which case the blockchain could not expand and remain transparent.

The blockchain technology is impressive due to its decentralized management, immutable records and the possibility to write smart contracts. Since they have these special features, intermediaries are unnecessary to make sure that policies cannot be altered [2]. Because of them, providing users with access to resources can become secure and completely automated, addressing the issues of equal treatment, transparency and trust.

Research is currently looking at how blockchain can improve access control in healthcare, financial services, smart cities and edge computing [3]. Such solutions hold a great potential but their structure, the degree of control they provide and their privacy options may vary dramatically. We also experience challenges in making interoperability, lowering latency and the capability to evaluate policies with a detailed and scalable level.

The review dissectors the current blockchain-based access control systems, which are categorized by their access model (RBAC, ABAC, CapBAC), the blockchain platform on which they rely (e.g., Ethereum and Hyperledger) as well as common privacy-enhancing approaches (decentralized identity and zero-knowledge proofs) [4]. We identify the strengths and weaknesses, underline the unknowns and suggest the avenues of developing secure and decentralized access structures in post-existing systems in Figure 1.

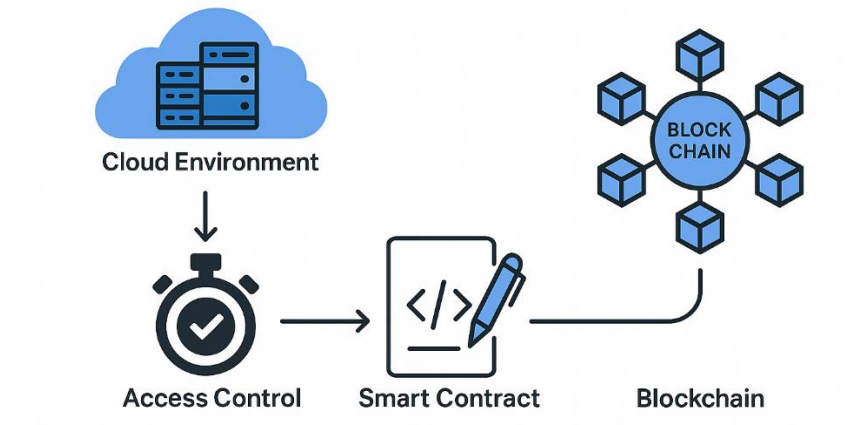

Figure 1. Cloud Environments in Blockchain-Driven Access Control

2. TAXONOMY OF BLOCKCHAIN-BASED ACCESS CONTROL SYSTEMS

To get better acquainted with the current access control using blockchain, approaches are categorized according to their access control model and the implementation platform they adhere to. Through this organization, the professionals can take time to research on technical design choices along with their impact on security, scalability and flexibility in Figure 2.

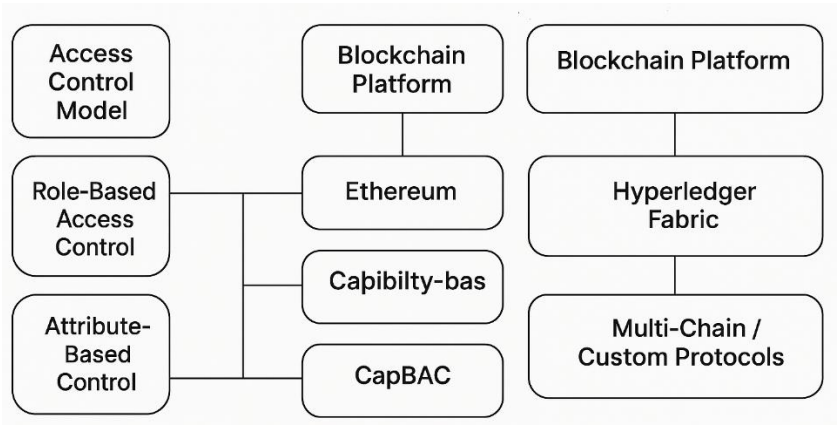

Figure 2. Taxonomy of Blockchain-Based Access Control Systems

2.1. By Access Control Model

2.1.1 Role-Based Access Control (RBAC)

RBAC is popular among enterprise systems due to the fact that roles are granted access, as opposed to assigning each individual user permission [5]. RBAC rules in the context of blockchain use are usually included in smart contracts, such that it becomes the case that roles are assigned and imposed automatically by the system. As an example, [1] implemented the RBAC system to Ethereum via smart contracts, such that the system is capable of managing the roles of users and their corresponding access privileges per transaction [6].

RBAC is much simpler in managing access to systems in a hierarchical environment, but this model does not scale quickly changing environments such as those present in IoT or multi-cloud systems. In most networks, the problem of keeping the role definitions current can cause problems in keeping everything up to date and managed.

2.1.2 Attribute-Based Access Control (ABAC)

Under ABAC, user identity, role, department, time and location are verified along with attributes about the resource to grant or reject access. Access decisions in blockchain systems are determined through evaluation of attribute expressions with smart contracts.

They used Hyperledger Fabric in their ABAC model (Sharma et al., 2021) such that access policies are stored in chaincode and verified against cryptographic attributes issued by a trusted entity. Under ABAC, it is possible to make smart and up-to-date access decisions without amending the contracts. Nonetheless, ABAC on a blockchain is considerably more compute-expensive to operate and necessitates the obscuration of sensitive data by privacy tools prior to being written there.

2.1.3 Capability-Based Access Control (CapBAC)

CapBAC shifts the emphasis on controlling access on the basis of identity to the permission assignments by means of tokens. Tokens or keys are presented to users, which enable them to demonstrate what permissions they possess, in attempt to access a resource. Smart contracts allow the users in CapBAC systems to issue, transfer and revoke such tokens which maximizes flexibility and decentralizes authority.

Through BlendCAC and CapChain, it has emerged that CapBAC is also able to take care of the problems in resource-constrained Internet of Things. As an example, BlendCAC uses blockchain to manage roles exchange and block functions in cases when the needs of users change. CapBAC can be easily integrated into applications that are based on a peer-to-peer framework since it has easy-to-implement and scalable controls. Operation of tokens and cancellation can be not easy in large environments and require in some cases some other coordination out of the network in Figure 3.

2.2. Blockchain Platform

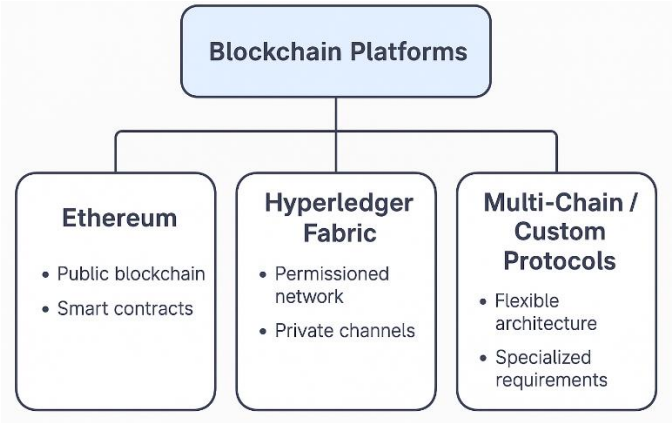

Figure 3. Blockchain Platform

2.2.1 Ethereum

Ethereum is number one in access control because its smart contracts are Turing complete (can do anything) and many developers work with it. Ethereum systems deal with controlled access through incorporating logic in smart contracts and anyone can audit all transactions. Ledgers contribute to making the system more reputable and transparent, but, on the other hand, because user attributes and access are stored on the blockchain, it may lead to certain privacy issues.

Ethereum is typically used as the main blockchain of open access systems which demand decentralized, traceable and censorship-resistant permission management on the public internet. Nevertheless, the number of transactions and gas costs is problematic as the figures of daily accesses by users grow.

2.2.2 Hyperledger Fabric

Hyperledger Fabric was developed by the Linux Foundation to be a modular, secure blockchain suitable to be used by both large enterprises and by groups attempting to collaborate. It can accommodate various consensus frameworks and stores information in privacy that qualifies it to be used in managing controlled access in sensitive zones.

As a chaincode technology, Fabric allows business to write smart contracts that constrain access but conceal their data to others. This can be illustrated by the fact that the access decisions in healthcare or financial sector can be done privately, and only the authorized people look at the ID of the people and the required attributes. However, since Fabric is complex to deploy and the ecosystem is significantly smaller than that of Ethereum, light and quick applications might not switch to it frequently.

2.2.3 Multi-Chain / Custom Protocols

Sometimes, developers and researchers create their own blockchain protocol or use MultiChain, Quorum or Polkadot to solve specific access control issues. They leave developers with a lot of freedom to implement how consensus is achieved, what kind of access is required and which data is exposed.

One of them is custom blockchains that PoA consensus mechanism to reduce access time and integrate with identity providers and external services. Some frameworks are designed to manage token-based CapBAC since the ground up and others can be connected to multiple blockchains. The designs are effective in maximizing efficiency, but they lack interoperability,

smaller developer communities, and they are costly to maintain. Ethereum, Hyperledger, and MultiChain comparative analysis is given in Table 1.

Table 1. Comparative Analysis of Ethereum, Hyperledger, and MultiChain

Criteria	**Ethereum**	**Hyperledger Fabric**	**MultiChain**
Platform Type	Public	Permissioned	Configurable
Consensus	Proof of Stake (PoS)	Pluggable	Configurable
Access Control Model Support	RBAC, ABAC, CapBAC	RBAC, ABAC, CapBAC	RBAC, ABAC, CapBAC
Performance	Moderate	High	Moderate to High
Privacy	Public by default	Private transactions	Controlled access
Scalability	Moderate	High	Moderate to High

2.3 Consensus Mechanisms

Access control in blockchain relies on consensus mechanisms which establish consensus amongst nodes regarding the state of the ledger, and is decentralized. Various consensus mechanisms significantly differ in terms of security, throughput, speed and outcome of the transactions processed. When Ethereum started, PoW was the primary option, but it consumes a lot of energy and is slower than other mechanisms to execute.$ With Ethereum 2.0, the consensus mechanism has switched to PoS, which is more appropriate to be used in access control applications because it consumes less energy. The enterprise platform Quorum relies on IBFT and Raft due to their quick private agreement. Polkadot and Cosmos enables more chains to safely connect and scale to a larger degree using NPoS and Tendermint BFT. PoW/PoS are suitable in open networks that can tolerate latency but Raft, PBFT and PoA are employed in fast and secure systems in enterprises or consortiums. To ensure its performance and reliability, the system has to reach to a consensus and offer proper access control.

3. IDENTITY AND AUTHENTICATION MECHANISMS

Identity and authentication are critical aspects when it comes to regulating access to a computing system [7], particularly in clouds and blockchain domains. They enable us to ensure that the person accessing a resource is who he/she claims to be and qualified to perform certain actions. As trustless and decentralized systems get increasingly popular, cryptographic and blockchain-based models are considered preferable to keep the information secure, maintain privacy and simplify the usage of systems in a combination.

3.1 Public-Key Cryptography

Public-key cryptography has become the primary defence in many modern cloud and blockchain networks to perform identity and authentication. To this end, each user or entity is assigned a cryptography key pair [8], consisting of a public key to interconnect everybody and a secret key used to sign transactions. With each request that the user makes, the system verifies the digital signature with the anticipated public key to determine the authenticity and identity of the requestor and thus no centralized authorities are necessary. Under the method, individuals are in charge of their own identities and no longer need to enter passwords. But cryptographic authentication does not provide an immediate revelation of the identity of the person in terms of name, role or organisation. Consequently, it does not scale to standardized access control scenarios, thus it needs new enhancements such as decentralized identity platforms.

3.2 Decentralized Identity (DID)

As a new solution to the issues of key-pair identity systems that have no human-friendly properties or simple cross-platform [9], DID has been presented. Using a DID, users can manage their identity themselves: they can generate, possess and control their own IDs and no longer need the services of central authorities. Such DIDs are typically paired with blockchain networks and all their data like public keys and service locations, are stored immutably, keeping them open and unchangeable. Each DID is associated with a DID Document, containing the primary cryptographic data, used in security and routing purposes. They may be stored on the blockchain, or referred to with external decentralized storage such as IPFS. The fact that DIDs are verifiable makes it possible to not reveal confidential information during the verification of the identity data. In this manner, a user would bind his or her cryptographic key to a DID and place it on a public ledger. Due to this DID, no combination of usernames and passwords is required, and secure authentication can occur everywhere, including across services, without exposing your privacy and keeping you in control.

3.3 Verifiable Credentials (VCs)

Although DIDs provide a method to control self-sovereign identity, they do not share by themselves information on what an individual does his /her qualification or his /her legal status. To address this gap Verifiable Credentials (VCs) have been added to assist in bridging this gap. VEs are digitally signed, which shows that the accuracy cannot be altered and is provided by organisations, called issuers, to a specific individual, typically the user. ID certificates are awarded to ascertain things like schooling, citizenship or employment status. As examples, a university can use a VC to validate a degree in computer science; a government agency can issue a document attesting the age or citizenship of a person [10]; an enterprise can distribute a VC naming a user as an Administrator.

VCs can be safely stored in a user digital identity wallet, either locally or in a decentralized cloud and verifiers can obtain access to them when required during the authentication or authorization steps. The verifier examines the signature and information regarding the issuer to examine that the credential is valid, unaltered and has been issued. VCs with DIDs enable users to establish facts, without communicating additional private information. It complements ABAC effectively, whereby dynamically attribute-based access is determined by attributes and not only by predetermined roles. Since credential issuance and verification is no longer centralized in a single center, VCs can be used to establish a reliable identity network which is accessible to all applications in contemporary clouds, edges and blockchains in Figure 4.

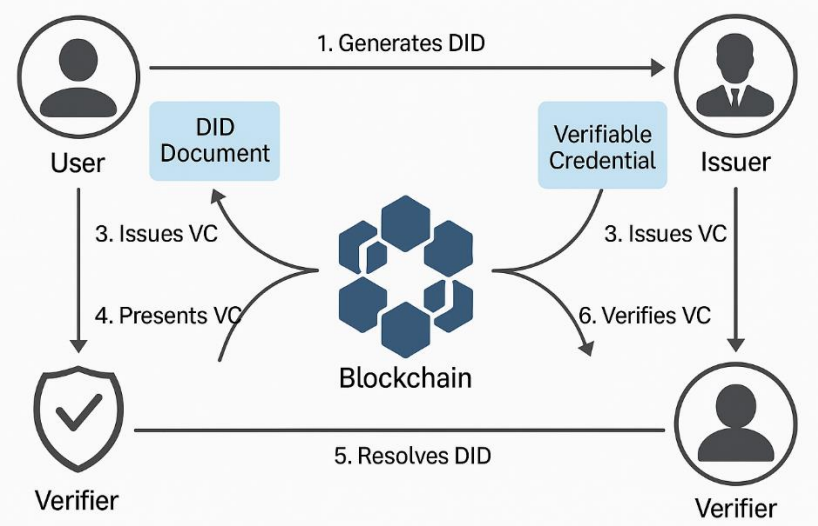

Figure 4. Identity Flow Using DIDs and VCs

3.4 Mathematical Modeling

The authorisation and authentication procedures are formalised by mathematical modelling. This entails using a set of formulas to define user roles, authorisations, and how they interact.

Smart Contract-Based Authorization

Let R be the set of roles, P be the set of permissions, and U be the set of users. Consider A as the authorisation matrix, where $A_{ur}$is equal to 1 if user u∈U holds role r∈R and 0 otherwise. These rules are enforced by the smart contract S.

Objective Function:

$$u \in U, r \in Rmin \sum_{u,r} A_{ur} \cdot C_r \quad (1)$$

Where the cost of assigning role rrr is represented by C_r.

The SSS smart contract guarantees:

$$S(u,r) = \begin{cases} 1 \; if \; A_{ur} = 1 \\ otherwise \\ 0 \end{cases} \quad (2)$$

This feature ensures safe and decentralised access control while reducing the overall cost of role assignments.

Secure Multi-Factor Authentication (MFA)

Let M [11] be the collection of authentication factors (password, biometric, token, etc.) for safe multi-factor authentication, and FFF be the set of users who successfully authenticated utilising at least two factors. If user u ∈ U uses factor m ∈ M [12] , define $X_{um} = 1$; if otherwise, define $X_{um} = 0$.

Objective Function:

$$u \in U, m \in Mmax \sum_{u,m} Xum \quad (3)$$

Subject to:

$$\sum_{m \in M} Xum \geq 2 \forall u \in U \quad (4)$$

Increasing the number of clients [13] who authenticate using two or more different factors is the aim. By confirming these elements before allowing access, the smart contract lowers the possibility of unwanted access in Figure 5 [14].

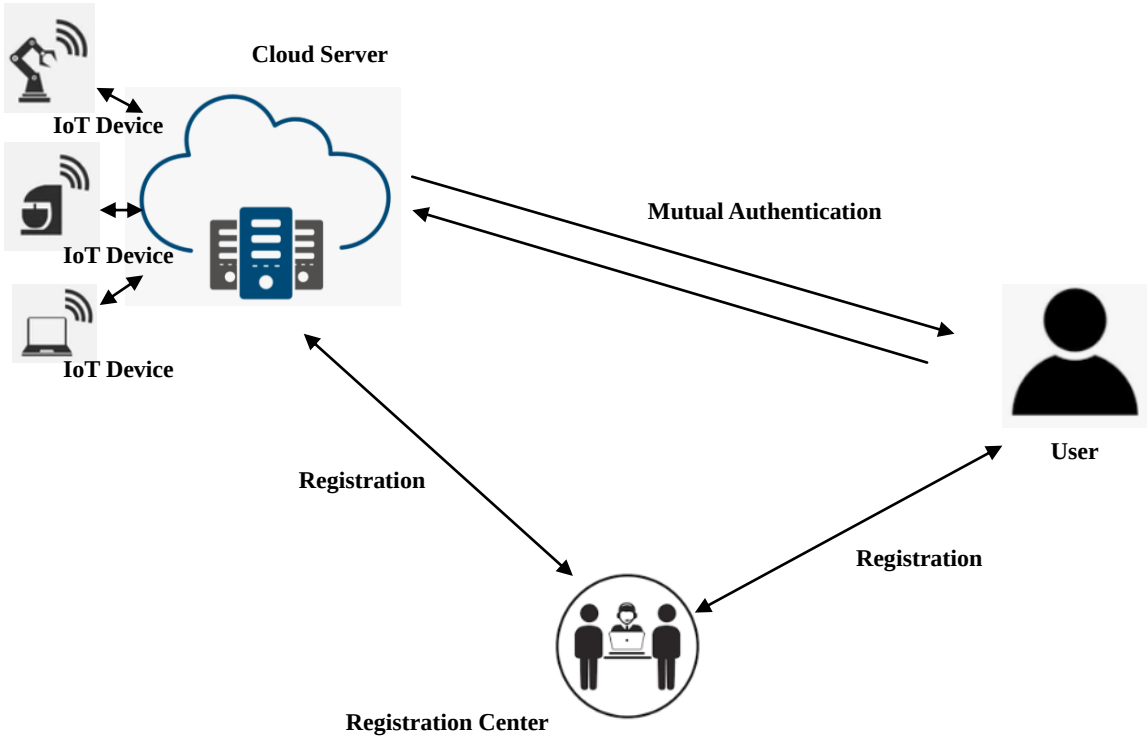

Figure 5. Research methodology

3.5 Secure Smart Contracts' Benefits in Cloud Environments

The rapid adoption of cloud computing has transformed the way organizations deploy, manage, and scale digital services. However [15] this transformation has also introduced significant security, trust, and governance challenges, particularly in multi-tenant and distributed cloud environments. Traditional cloud security mechanisms rely heavily on centralized access control, trusted third parties, and manual policy enforcement, which can become bottlenecks and points of failure. In this context, secure smart contracts deployed on blockchain platforms have emerged as a promising solution for enhancing security, transparency, and automation in cloud environments.

One of the most significant advantages of secure smart contracts is their ability to provide tamper-resistant and immutable execution of security policies. Smart contracts are deployed on blockchain networks where transaction records and contract logic are protected by cryptographic hashing and consensus mechanisms. Once deployed, the contract code cannot be altered without network-wide agreement, ensuring that access control rules, authorization conditions, and service-level agreements remain intact. This immutability significantly reduces risks associated with insider threats, configuration tampering, and unauthorized policy changes, which are common vulnerabilities in centralized cloud infrastructures.

Secure smart contracts also enable a decentralized trust model, which is particularly beneficial in cloud environments involving multiple stakeholders, such as cloud service providers, users, enterprises, and third-party vendors. Instead of relying on a single centralized authority to authenticate users and authorize actions, smart contracts enforce trust through distributed consensus. This eliminates single points of failure and reduces reliance on intermediaries, thereby increasing system robustness and trustworthiness. In federated or hybrid cloud settings, this decentralized trust model facilitates secure collaboration among entities that may not fully trust each other.

Another major advantage lies in the automation of access control and policy enforcement. Smart contracts are self-executing programs that automatically enforce predefined rules when specified conditions are met. In cloud environments, this capability enables real-time, rule-based access control without human intervention. For example, access permissions can be automatically granted or revoked based on user attributes, service usage patterns, or contractual obligations. This automation minimizes human error, reduces administrative overhead, and ensures consistent enforcement of security policies across distributed cloud services.

Transparency and auditability are also substantially enhanced through the use of secure smart contracts. Every transaction and access request processed by a smart contract is recorded on an immutable blockchain ledger, creating a permanent and verifiable audit trail. This feature is particularly valuable for regulatory compliance, forensic analysis, and accountability in cloud environments. Organizations can easily verify who accessed which resources, under what conditions, and at what time, without relying on centralized log management systems that may be vulnerable to manipulation or loss.

Secure smart contracts further contribute to fraud prevention and misuse detection. By enforcing strict rule-based execution and cryptographic verification of transactions, smart contracts can effectively prevent unauthorized actions and malicious behaviors. Any attempt to violate predefined access policies is automatically rejected by the contract logic, ensuring proactive security enforcement rather than reactive detection. This capability is especially important in sensitive cloud applications such as healthcare, finance, and government services, where unauthorized access can have severe consequences.

Another key advantage is the support for fine-grained and flexible access control mechanisms. Smart contracts can implement a wide range of access control models, including role-based access control (RBAC), attribute-based access control (ABAC), and capability-based access control. These models allow access decisions to be made based on dynamic parameters such as user roles, contextual attributes, service states, and environmental conditions. This flexibility enables more precise and adaptive security policies compared to static, centralized access control systems.

Interoperability across distributed and heterogeneous cloud platforms is also enhanced through blockchain-enabled smart contracts. In multi-cloud and cross-domain environments, smart contracts can act as trusted intermediaries that enforce uniform security policies across different cloud providers. This capability simplifies cross-platform access management, data sharing, and service orchestration while maintaining consistent security guarantees. As cloud ecosystems become increasingly interconnected, this interoperability becomes a critical requirement.

From an operational perspective, secure smart contracts contribute to cost reduction and efficiency improvements**.** By automating authentication, authorization, and policy enforcement processes, organizations can reduce manual administrative tasks and reliance on third-party verification services. Over time, this automation leads to lower operational costs and improved

scalability, particularly in large-scale cloud deployments. Scalability is another important benefit of smart contract–based security mechanisms. Once deployed, smart contracts can be replicated and executed across multiple blockchain nodes, enabling consistent enforcement of security policies at scale. This distributed execution model aligns well with the elastic and scalable nature of cloud computing, allowing security mechanisms to grow alongside cloud infrastructure without significant redesign.

Privacy protection is also enhanced through the integration of advanced cryptographic techniques within smart contracts. Mechanisms such as zero-knowledge proofs, decentralized identifiers, and selective disclosure protocols can be incorporated to protect sensitive user data while maintaining verification and accountability. This balance between transparency and privacy is particularly important in cloud environments that handle personal or confidential information.

Secure smart contracts also enable real-time monitoring and enforcement of cloud security policies. Access requests and transactions are validated instantly against contract logic, allowing immediate detection and prevention of policy violations. This real-time capability improves the responsiveness of cloud security systems and reduces the window of opportunity for attackers.

Finally, the decentralized and fault-tolerant nature of blockchain-based smart contracts enhances the reliability and resilience of cloud security infrastructures. Even if individual nodes or components fail, the distributed ledger continues to operate, ensuring uninterrupted access control and service availability. This resilience is critical for mission-critical cloud applications that require high availability and robustness.

In summary, secure smart contracts offer a comprehensive set of advantages for cloud environments, including enhanced security, decentralized trust, automated enforcement, transparency, scalability, privacy protection, and operational efficiency. By addressing many of the limitations of traditional centralized security mechanisms, smart contracts provide a powerful foundation for next-generation cloud security architectures. As cloud systems continue to evolve toward more distributed and collaborative models, the role of secure smart contracts is expected to become increasingly central in ensuring trustworthy and resilient cloud computing ecosystems.

4. INTEGRATION OF PRIVACY AND SECURITY TECHNIQUES

Since cloud technology and decentralized identity systems handle very sensitive data, ensuring privacy is maintained in Figure 4, user authentication and access are granted is now of high importance. Public-key cryptography, DIDs and Verifiable Credentials assist in securing the data, but rarely assist in safeguarding privacy in verification flows. Therefore, emerging systems are incorporating novel methodologies such as Zero-Knowledge Proofs (ZKPs), Homomorphic Encryption and Secure Multi-Party Computation (SMPC) into their framework.

Due to ZKPs, users can provide evidence of information such as age or role without revealing that information, improving the security of attribute-based permission models. Homomorphic Encryption allows cloud providers to operate on encrypted data due to security reasons. Due to SMPC, several parties can computally collaborate on their confidential inputs without any party observing the confidential data.

On which note, despite the addition of such techniques, latency can be introduced as well as the workload on the computer, which could be why they do not always play nicely with real-time applications. Due to the increased number of rules and the desire of people to have more control over their data, privacy-enhancing technologies become important components of secure

and contemporary cloud and identity systems. Advances in cryptography and associated systems are extremely significant to increase the use of crypto assets.

5. CHALLENGES IDENTIFIED

Despite the promising perspective of access control systems based on blockchain, they still have certain problems that do not allow them to be used practically. Because the network is not capable of processing a high number of transactions simultaneously, scaling is a primary concern regarding the decisions made by blockchains during a high-stress situation. The on-chain checks introduce further delays, which complicate access control in real time. In addition to that, it is difficult, prone to errors, and reduces adaptation capabilities over time to establish and implement elaborate access control rules in smart contracts. Different blockchain platforms can hardly be compatible with one another due to the difference in the identity and access control rules. These kinds of problems imply that we need to continue working on new scalable networks, hybrid on-chain/off-chain systems and settled protocols of greater usage.

6. FUTURE DIRECTIONS

Any subsequent advancements in blockchain-based access control systems should be done in the efforts to scale them up, make them flexible and capable of interconnecting with various other networks. We can offload a lot of the transactions into those layers by integrating Layer-2, which can aid in solving the bottlenecks of blockchain and reduce traffic. Policy engines with AI will adjust access control rules in real time due to their learning capabilities, which will make things more secure and flexible. They require the utilization of cross-blockchain access procedures, which provide that the authorization between the blockchain networks of different types is secure and convenient. Research on privacy-utility trade-off models will be useful in enhancing the utility of a system without interfering with the security of the data, especially in situations that attribute verification is employed. Finally, regarding smart contract access control, the presence of interfaces of the same kind will standardize platforms, and it will be less complex to implement policies that, in turn, will contribute to the popularization of the use of decentralized access systems.

7. CONCLUSION

In blockchain, access control in decentralized systems and cloud-connected systems is improved. The paper examined RBAC, ABAC and CapBAC models and elaborated on their limitations, gaps and privacy issues in the existing blockchain platforms. The considered DIDs and VCs based on ZKPs and SMPC, enhance security in access and safeguard the privacy of users. Despite this significant development, scaling, lowering latency and getting cryptocurrencies to interact with one another remains challenging. The efforts required to realize secure and flexible management of user access in the next-generation cloud should stay on Layer-2 options, uniform policy interfaces and supporting AI-powered systems.

REFERENCES

[1] Li, H., Dai, Y., Tian, Z., Yu, R., & Wang, X. (2020). Achieving Secure and Efficient Dynamic Access Control with Blockchain-Based Smart Contracts. IEEE Access, 8, 90638–90652. https://doi.org/10.1109/ACCESS.2020.2994440

[2] Sharma, P. K., Park, J. H., & Moon, S. Y. (2021). A Secure and Distributed Framework for Access Control Using Blockchain and Attribute-Based Encryption. IEEE Access, 9, 23683–23695. https://doi.org/10.1109/ACCESS.2021.3056441

[3] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the Internet of Things. IEEE Internet of Things Journal, 6(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705

[4] Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2017). FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things. Security and Communication Networks, 2017, 1–14. https://doi.org/10.1155/2017/7095071

[5] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27

[6] Dunphy, P., &Petitcolas, F. A. (2018). A First Look at Identity Management Schemes on the Blockchain. IEEE Security & Privacy, 16(4), 20–29. https://doi.org/10.1109/MSP.2018.3111247

[7] Hardjono, T., & Smith, N. (2020). Decentralized Trusted Identity. The Internet Protocol Journal, 23(3), 4–17. [Cisco Publication]

[8] Liu, Y., Zhang, M., Pang, Y., & Wang, Y. (2020). Blockchain-based Access Control System for Edge Devices in Smart Manufacturing. IEEE Access, 8, 4534–4543. https://doi.org/10.1109/ACCESS.2020.2965678

[9] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[10] Halpin, H., & Piekarska, M. (2018). Introduction to Security and Privacy on the Blockchain. In 2018 IEEE European Symposium on Security and Privacy Workshops (pp. 1–3). IEEE. https://doi.org/10.1109/EuroSPW.2018.00013

[11] Halily, R., & Shen, M. (2024). Directing techniques for high frequency antennas for use in next-generation telecommunication countries. National Journal of Antennas and Propagation, 6(1), 49–57.

[12] Manaa Barhoumi, E., Charabi, Y., & Farhani, S. (2023). FPGA Application: Realization of IIR Filter Based Architecture. Journal of VLSI Circuits and Systems, 5(2), 29–35. https://doi.org/10.31838/jvcs/05.02.05

[13] Alatawi, M. N. (2025). Blockchain-Driven Smart Contracts for Advanced Authorization and Authentication in Cloud Security. *Electronics*, *14*(15), 3104.

[14] Dar, A. B., Lone, A. H., Naaz, R., Baba, A. I., & Wu, F. (2022). Blockchain Driven Access Control Mechanisms, Models and Frameworks: A Systematic Literature Review. *Journal of Information Security and Cybercrimes Research*, *5*(1), 05-34.

[15] Khayer, B., Mirzaei, S., Alavizadeh, H., & Salehi Shahraki, A. (2025). Blockchain for Secure IoT: A Review of Identity Management, Access Control, and Trust Mechanisms. *IoT*, *6*(4), 65.