International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

DESIGN OF A BLOCKCHAIN-BASED ACCESS CONTROL ARCHITECTURE FOR SOFTWARE-DEFINED CLOUD NETWORKS

Moorthy K[1], Gavaskar S[2]
[1]*Research Scholar, Department of Computer Applications, Bharathiar University, Coimbatore*
[2]*Assistant Professor, Department of Computer Applications, Bharathiar University, Coimbatore*

Abstract—Cloud computing and Software-Defined Networking (SDN) have emerged as key technologies for building scalable, flexible, and programmable network infrastructures. The separation of the control and data planes in SDN enables centralized network management and dynamic resource provisioning; however, conventional access control mechanisms in Software-Defined Cloud Networks (SDCNs) remain largely dependent on centralized trust authorities, making them vulnerable to insider attacks, privilege escalation, policy manipulation, and single points of failure [1], [4], [6], [21]. Recent studies have demonstrated the potential of blockchain technology to provide decentralized trust, immutable audit trails, and transparent policy enforcement for cloud and distributed systems [3], [5], [8], [14].

This paper proposes a blockchain-based access control architecture that integrates a permissioned Hyperledger Fabric blockchain with SDN controllers to provide secure, decentralized, and tamper-resistant access management for cloud environments. The proposed framework employs smart contracts to automate authentication, authorization, policy verification, and audit logging processes while supporting fine-grained access control over virtualized cloud resources [7], [12], [13], [22]. In addition, the architecture incorporates Zero Trust principles to ensure continuous verification of access requests and enhance resilience against unauthorized access attempts [8], [14].

A prototype implementation was developed using Mininet, OpenFlow-enabled switches, and Hyperledger Fabric to evaluate the effectiveness of the proposed solution [13], [21], [23]. Experimental results demonstrate that the framework significantly improves security, transparency, auditability, and policy management while introducing only minimal latency overhead compared with conventional SDN-based access control mechanisms [15]–[20].

Furthermore, security analysis indicates enhanced resistance against insider threats, policy tampering attacks, and unauthorized privilege escalation through immutable blockchain records and decentralized policy verification [16], [18], [20], [24]. The proposed architecture offers a practical and scalable solution for securing dynamic, multi-tenant, and software-defined cloud infrastructures and provides a foundation for future blockchain-enabled Zero Trust cloud environments [14], [22], [25].

Keywords—Blockchain, Software-Defined Networking, Cloud Security, Access Control, Smart Contracts, Hyperledger Fabric, Zero Trust Architecture, Software-Defined Cloud Networks.

I. INTRODUCTION

Cloud computing has become a cornerstone of modern digital infrastructures, providing on-demand access to computing resources, scalable storage, and flexible service delivery for enterprises and individuals. The widespread adoption of cloud services has significantly transformed the way organizations deploy and manage applications, enabling cost-effective and elastic computing environments [1], [5]. However, the increasing complexity of cloud infrastructures and the growing volume of interconnected devices have introduced new security challenges, particularly in authentication, authorization, and access management [1], [2], [22].

Software-Defined Networking (SDN) has emerged as a promising networking paradigm that separates the control plane from the data plane, enabling centralized network control, programmability, and dynamic resource management [11], [21]. Through centralized controllers, SDN facilitates efficient traffic engineering, network virtualization, and rapid policy deployment, making it an attractive solution for cloud computing environments. Nevertheless, the centralized nature of SDN controllers introduces security concerns, including controller compromise, unauthorized access, policy manipulation, and single points of failure [4], [6], [19].

Access control remains one of the most critical security requirements in Software-Defined Cloud Networks (SDCNs). Traditional access control models, including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), rely heavily on centralized authorities for policy management and decision making [1], [2]. Although these approaches provide structured authorization mechanisms, they often suffer from limited transparency, scalability constraints, and vulnerability to insider attacks and administrative misconfigurations in distributed cloud environments [3], [22]. As cloud infrastructures become increasingly dynamic and multi-tenant, there is a growing need for decentralized, auditable, and fine-grained access control solutions.

Blockchain technology has emerged as a disruptive technology capable of establishing decentralized trust in distributed systems. Originally introduced through Bitcoin by Nakamoto [9], blockchain provides immutable ledgers, cryptographic integrity, consensus-based validation, and transparent transaction recording. Subsequent studies have demonstrated the applicability of blockchain beyond cryptocurrency, particularly in cloud security, access control, and distributed resource management [5], [10], [14], [23]. The integration of smart contracts further enables automated policy enforcement and trustworthy access verification without dependence on centralized intermediaries [7], [13].

Recent research has explored the integration of blockchain and SDN to enhance network security and access management. Blockchain-assisted SDN frameworks have been proposed to secure east-west communications, strengthen controller interactions, and provide decentralized policy verification mechanisms [4], [15]. B-DAC introduced a decentralized blockchain-based access control framework for securing SDN northbound interfaces [16], while SBAC-SDN enhanced scalability through multi-controller blockchain-assisted access control mechanisms [17]. Chattaraj et al. proposed a blockchain-based access control scheme for SDN environments that improved policy integrity and authorization transparency [18]. Additional studies have focused on secure REST API access management and blockchain-enabled SDN security architectures for cloud and IoT environments [19], [20]. Despite these advancements, existing solutions often focus on specific SDN components or IoT scenarios and provide limited support for comprehensive access control management in software-defined cloud infrastructures.

Furthermore, emerging security paradigms such as Zero Trust Architecture emphasize continuous verification and least-privilege access principles for distributed environments [8]. Blockchain technology complements Zero Trust by providing immutable policy storage, decentralized trust establishment, and transparent auditing capabilities [14], [24], [25]. However, the integration of blockchain-enabled Zero Trust access control within Software-Defined Cloud Networks remains insufficiently explored.

To address these limitations, this paper proposes a blockchain-based access control architecture for Software-Defined Cloud Networks that combines the programmability of SDN with the decentralized trust and immutability of blockchain technology. The proposed framework employs Hyperledger Fabric as a permissioned blockchain platform to support secure authentication, authorization, policy management, and audit logging through smart contracts [13]. By integrating blockchain with SDN controllers, the framework enables transparent, tamper-resistant, and scalable access management while minimizing reliance on centralized trust authorities.

The major contributions of this work are summarized as follows:

- A blockchain-supported access control architecture for Software-Defined Cloud Networks is proposed to enhance security, transparency, and trust management.
- A permissioned Hyperledger Fabric blockchain is integrated with SDN controllers to provide decentralized policy verification and immutable audit logging.
- Smart contract mechanisms are designed to automate authentication, authorization, and policy enforcement processes.

• A comprehensive security analysis is conducted to evaluate resistance against insider threats, policy tampering attacks, and unauthorized access attempts.
• Experimental evaluation using Mininet and Hyperledger Fabric demonstrates the feasibility, scalability, and effectiveness of the proposed framework for modern cloud infrastructures.

II. RELATED WORK

Access control remains a fundamental security requirement in cloud computing, Software-Defined Networking (SDN), and Internet of Things (IoT) environments. Traditional access control mechanisms, including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), have been widely adopted because of their simplicity and policy management capabilities. However, these approaches rely heavily on centralized authorization servers, which can become bottlenecks and single points of failure in large-scale distributed environments [1], [2]. Furthermore, centralized architectures often face challenges related to scalability, transparency, trust management, and resistance to insider attacks.

Recent advances in blockchain technology have motivated researchers to explore decentralized access control frameworks for cloud and distributed systems. Blockchain provides immutable record keeping, distributed trust establishment, cryptographic security, and transparent transaction validation, making it an attractive platform for access control applications [9], [10], [14]. Several surveys have highlighted the potential of blockchain-enabled access control mechanisms in cloud computing, IoT networks, and distributed infrastructures, demonstrating improved accountability, auditability, and tamper resistance compared with conventional approaches [1], [2], [5], [25].

In cloud computing environments, blockchain-based access control solutions have been proposed to eliminate dependence on centralized authorities and enhance trust management. Khan et al. [3] introduced a blockchain-supported cloud access control framework that improves transparency and policy verification. Similarly, Fang et al. [22] proposed a fine-grained blockchain-based access control mechanism for cloud storage systems, enabling secure resource sharing while preserving data integrity. These studies demonstrate the effectiveness of blockchain in enforcing decentralized authorization policies; however, they do not specifically address the challenges associated with software-defined cloud infrastructures.

The emergence of SDN has significantly transformed network management by separating the control plane from the data plane and enabling centralized programmability through SDN controllers [11], [21]. Although SDN improves network flexibility and resource utilization, the centralized controller architecture introduces new security risks, including controller compromise, unauthorized access, malicious application behavior, and policy manipulation attacks [4], [19]. Consequently, securing access control mechanisms within SDN environments has become an important research area.

Several researchers have investigated blockchain-assisted security frameworks for SDN. Alrashede et al. [4] proposed a blockchain-enabled mechanism to secure east-west communications in heterogeneous SDN environments. Chavan et al. [6] developed BCSDNCC, a blockchain-integrated SDN framework for enhancing security in cloud and IoT networks. Khalid et al. [7] further explored the use of smart contracts for automating access control decisions in SDN-based IoT systems. These studies demonstrate that blockchain can improve trust and policy integrity within SDN architectures.

More recently, dedicated blockchain-based access control schemes for SDN have been proposed. Duy et al. [16] introduced B-DAC, a decentralized access control framework that secures the SDN northbound interface using blockchain technology. Chattaraj et al. [18] proposed a blockchain-based access control scheme for software-defined networks that enhances authorization transparency and prevents unauthorized policy modifications. Zainal et al. [17] developed SBAC-SDN, which improves scalability through a multi-controller architecture and load-balancing mechanisms. Similarly, Hu et al. [19] proposed SEAPP, a secure application management framework that employs REST API access control for SDN-enabled cloud environments. These solutions provide significant improvements in access control security; however, most focus on specific SDN components rather than comprehensive cloud resource protection.

Blockchain-SDN integration has also been explored for cloud and industrial environments. Abd El-Latif et al. [15] proposed a Blockchain-SDN-based secure architecture for smart industrial IoT applications, demonstrating the feasibility of combining blockchain and SDN to improve trust management and communication security. Rahman et al. [20] presented a distributed blockchain-enabled SDN architecture that enhances cloud security in IoT environments. These studies confirm the effectiveness of blockchain-assisted SDN architectures but provide limited support for fine-grained access control and audit management in multi-tenant cloud infrastructures.

In addition to blockchain-enabled security mechanisms, researchers have investigated distributed trust models and Zero Trust architectures for cloud systems. Gai et al. [8] proposed a blockchain-based access control framework for Zero Trust cross-organizational data sharing, highlighting the importance of continuous verification and decentralized trust. Hyperledger Fabric has emerged as a preferred permissioned blockchain platform for implementing enterprise-grade access control systems because of its support for smart contracts, privacy-preserving channels, and efficient consensus mechanisms [13], [23]. These characteristics make it particularly suitable for Software-Defined Cloud Networks where secure and low-latency authorization decisions are required.

Despite the significant progress achieved by existing studies, several research gaps remain. First, many blockchain-based access control solutions focus primarily on IoT or cloud storage environments rather than software-defined cloud infrastructures. Second, existing SDN security frameworks often address controller communication security without providing integrated authentication, authorization, policy management, and auditing mechanisms. Third, limited research has explored the combination of permissioned blockchain platforms, smart contracts, and SDN controllers to support scalable and transparent access control in multi-tenant cloud environments.

To address these limitations, this paper proposes a blockchain-based access control architecture for Software-Defined Cloud Networks that integrates Hyperledger Fabric, SDN controllers, and smart contracts to provide decentralized policy enforcement, immutable audit logging, and fine-grained access management. The proposed framework aims to enhance transparency, security, and scalability while maintaining acceptable performance overhead in dynamic cloud environments.

III. PROBLEM STATEMENT AND MOTIVATION

Software-Defined Cloud Networks (SDCNs) combine the scalability of cloud computing with the programmability and centralized control capabilities of Software-Defined Networking (SDN). While this integration enables efficient resource utilization, dynamic network management, and flexible service provisioning, it also introduces significant security and access-control challenges [11], [21]. In most existing cloud infrastructures, access control decisions are managed through centralized authentication and authorization servers, creating potential single points of failure and increasing vulnerability to insider attacks, privilege escalation, unauthorized access, and policy manipulation [1], [2], [6].

Traditional access control mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) have been widely adopted in cloud environments because of their structured authorization models [1], [2]. However, these approaches face several limitations in modern software-defined cloud infrastructures. First, centralized policy repositories and authorization servers may become performance bottlenecks when handling large numbers of users, devices, and virtual resources. Second, maintaining consistency and transparency across distributed cloud environments is challenging, particularly in multi-tenant deployments where access policies frequently change [3], [22]. Third, existing systems often provide limited auditability, making it difficult to verify policy enforcement actions and detect malicious administrative activities [14].

The centralized architecture of SDN further amplifies these challenges. SDN controllers are responsible for managing network policies and forwarding decisions across the infrastructure.

Consequently, a compromised controller or malicious application can potentially manipulate network configurations, bypass security policies, or disrupt service availability [4], [19]. Although several SDN security mechanisms have been proposed, many focus primarily on securing controller communications and network traffic rather than providing comprehensive and decentralized access control management [6], [15], [20].

Recent studies have investigated blockchain technology as a mechanism for establishing decentralized trust and improving security in distributed systems [9], [10], [14]. Blockchain provides an immutable ledger, consensus-based validation, cryptographic integrity, and transparent transaction recording, enabling secure and tamper-resistant management of access control policies [5], [23]. Furthermore, smart contracts allow automatic execution of authentication and authorization rules without requiring continuous intervention from centralized administrators [7], [13]. These characteristics make blockchain particularly attractive for cloud and SDN environments where trust must be established among multiple stakeholders.

Several blockchain-based access control solutions have been proposed for cloud computing, IoT networks, and SDN infrastructures [3], [7], [8], [16], [18]. For example, B-DAC introduced decentralized access control for SDN northbound interfaces using blockchain technology [16], while Chattaraj et al. proposed a blockchain-assisted authorization framework for software-defined networks [18]. Similarly, blockchain-SDN architectures have been explored to improve communication security and trust management in cloud and industrial IoT environments [15], [20]. Despite these advances, existing approaches often focus on specific components of SDN architectures, provide limited support for fine-grained cloud resource authorization, or lack comprehensive auditing and policy management capabilities suitable for dynamic multi-tenant cloud infrastructures.

In addition, emerging Zero Trust security models require continuous verification of users, devices, and services before granting resource access [8]. Implementing such a model within SDCNs requires a trustworthy and decentralized mechanism capable of maintaining immutable access policies, supporting real-time authorization decisions, and providing transparent auditing capabilities. Existing centralized access control systems are often inadequate for meeting these requirements [14], [24], [25].

Therefore, there is a need for a secure, scalable, and transparent access control framework that can eliminate reliance on centralized trust authorities while supporting dynamic policy management in Software-Defined Cloud Networks. The proposed research addresses this challenge by integrating a permissioned blockchain platform with SDN controllers and smart contracts to establish decentralized trust, automate authorization processes, and provide immutable audit trails for access control operations [13], [16], [17].

A. Research Gap

Based on the literature review, the following research gaps are identified:

Existing cloud access control systems rely heavily on centralized trust models, leading to security vulnerabilities and management bottlenecks [1], [3].

Most blockchain-enabled access control solutions focus on IoT or cloud storage environments and do not adequately address Software-Defined Cloud Networks [2], [22], [25].

Current SDN security frameworks primarily secure controller communications but provide limited support for decentralized policy management and auditing [4], [19].

Few existing solutions integrate permissioned blockchain platforms, smart contracts, and SDN controllers into a unified framework for cloud access control [15], [16], [18].

Support for Zero Trust principles, continuous verification, and immutable auditability remains insufficient in many existing SDCN access control solutions [8], [14].

B. Motivation and Objectives

The primary motivation of this work is to leverage the decentralized trust and immutability properties of blockchain technology to overcome the limitations of traditional access control

Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

systems in Software-Defined Cloud Networks. By integrating Hyperledger Fabric with SDN controllers and smart contracts, the proposed framework aims to:

- Eliminate single points of failure in access-control decision making.
- Provide transparent and tamper-resistant policy management.
- Enable automated authentication and authorization through smart contracts.
- Support fine-grained and scalable access control for multi-tenant cloud environments.
- Improve auditability, accountability, and regulatory compliance through immutable logging.
- Facilitate secure implementation of Zero Trust access control principles in software-defined cloud infrastructures.

The proposed framework is designed to provide a practical and scalable solution for securing next-generation cloud environments while maintaining acceptable performance overhead and operational flexibility.

IV. PROPOSED ARCHITECTURE AND DESIGN

This section presents the proposed blockchain-based access control architecture for Software-Defined Cloud Networks (SDCNs). The architecture integrates Software-Defined Networking (SDN), permissioned blockchain technology, and smart contracts to provide decentralized, transparent, and tamper-resistant access control. Unlike traditional cloud access-control systems that depend on centralized authorization servers, the proposed framework distributes trust across blockchain peers while maintaining the programmability and flexibility of SDN controllers [4], [6], [15], [20].

The design aims to achieve the following objectives:

- Decentralized access-control management.
- Fine-grained authorization of cloud resources.
- Immutable audit logging and accountability.
- Automated policy enforcement using smart contracts.
- Scalability for multi-tenant cloud environments.
- Support for Zero Trust security principles [8].

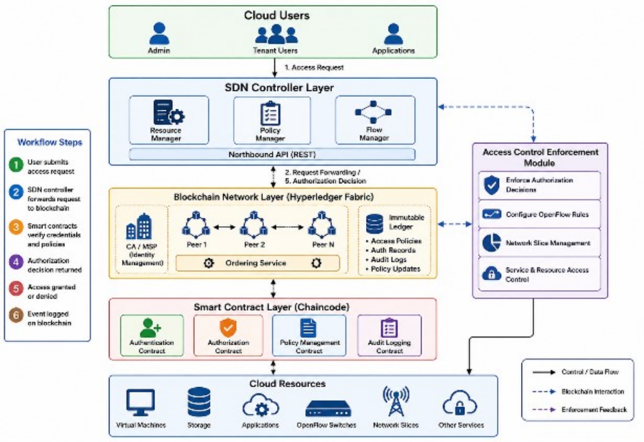
A. Architecture Overview

The proposed architecture consists of four major components:

- SDN Controller Layer
- Blockchain Network Layer
- Smart Contract Layer
- Access Control Enforcement Layer

The interaction among these components enables secure authentication, authorization, policy verification, and auditing of all access-control operations within the cloud infrastructure.

Figure 1. Proposed Blockchain-Based Access Control Architecture



DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

The architecture combines centralized network programmability with decentralized trust management, thereby addressing the security limitations of conventional SDN-based cloud infrastructures [15], [16], [18].

B. SDN Controller Layer

The SDN controller serves as the central management entity responsible for network orchestration, traffic engineering, and resource allocation [11], [21]. It maintains a global view of the network and dynamically configures forwarding rules on OpenFlow-enabled switches.

In the proposed framework, the controller does not independently make authorization decisions. Instead, it acts as an intermediary between users and the blockchain network. Whenever an access request is received, the controller forwards the request to the blockchain layer for verification before enforcing any policy [4], [6], [19].

The controller performs the following functions:

- Resource discovery and management.
- Access-request forwarding.
- Flow-rule installation.
- Enforcement of authorization decisions.
- Policy synchronization with blockchain records.

This approach reduces the risk of controller compromise and unauthorized policy modifications [4], [19].

C. Blockchain Network Layer

A permissioned blockchain network based on Hyperledger Fabric is used to establish decentralized trust among participating entities [13]. Unlike public blockchains, permissioned blockchain systems provide controlled membership, lower latency, improved scalability, and enhanced privacy, making them suitable for enterprise cloud environments [13], [23].

The blockchain ledger stores:

- User identities.
- Access-control policies.
- Authorization transactions.
- Policy updates.
- Audit logs.

Each transaction undergoes validation through consensus mechanisms before being permanently recorded in the ledger. Consequently, policy modifications and authorization records become tamper-resistant and auditable [5], [14], [24].

The decentralized nature of the blockchain eliminates single points of failure that commonly affect centralized authorization systems [1], [5].

D. Smart Contract Layer

Smart contracts (chaincode) automate authentication and authorization decisions based on predefined security policies [3], [7], [13].

The proposed smart contract framework consists of four primary modules:

1) User Registration Module

This module registers users and associates their identities with blockchain credentials.

RegisterUser(UserID,Role,Attributes)

2) Authentication Module

This module validates user credentials and verifies identity ownership.

Authenticate(UserID, Credentials)

3) Authorization Module

This module evaluates access policies and determines whether a requested operation should be permitted.

Authorize(UserID, ResourceID, Action)

4) Audit Module

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

This module records all access-related events on the blockchain ledger.

LogAccess(UserID,ResourceID, Decision, Timestamp)

By automating authorization decisions, smart contracts eliminate manual policy enforcement and reduce the possibility of human errors or malicious administrative actions [7], [16].

E. Access Control Enforcement Layer

The Access Control Enforcement Module is responsible for implementing authorization decisions received from the blockchain layer. Once an authorization request is approved, the SDN controller dynamically installs OpenFlow rules and network policies that permit access to the requested cloud resource [21].

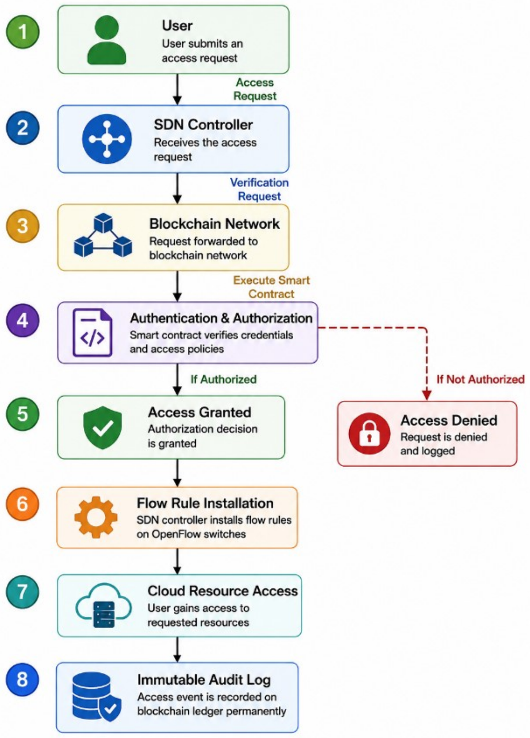
The module supports:

- Virtual machine access control.
- Cloud storage authorization.
- Application-level permissions.
- Network slice isolation.
- Multi-tenant resource protection.

If access is denied, corresponding network flows are blocked and logged for future auditing purposes [16], [18].

F. Access Request Workflow

Figure 2. Access Request Workflow



The workflow consists of the following steps:

- A user submits an access request for a cloud resource.
- The SDN controller receives and forwards the request to the blockchain network.
- Smart contracts verify user identity and evaluate access-control policies.
- The blockchain network generates an authorization decision.
- The decision is returned to the SDN controller.
- The controller installs corresponding flow rules and network policies.
- Access is granted or denied.
- The transaction is permanently recorded on the blockchain ledger.

DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

- This process ensures transparent, decentralized, and verifiable access-control operations [3], [7], [18].

G. Security Analysis of the Architecture

The proposed architecture addresses several critical security challenges in Software-Defined Cloud Networks.

1) Resistance to Single Points of Failure

Unlike centralized authorization servers, access-control records are distributed across multiple blockchain peers, ensuring service continuity even if individual nodes fail [5], [13].

2) Protection Against Insider Attacks

All authorization decisions and policy updates are immutably recorded on the blockchain, making unauthorized modifications detectable and traceable [14], [25].

3) Tamper-Resistant Auditability

Blockchain consensus mechanisms ensure that audit logs cannot be altered without network-wide agreement, improving accountability and regulatory compliance [5], [14].

4) Zero Trust Compatibility

The architecture supports continuous verification and decentralized trust establishment, aligning with modern Zero Trust security principles [8].

5) Fine-Grained Access Control

Smart contracts enable dynamic policy enforcement based on user attributes, resource characteristics, and contextual information, thereby supporting highly granular authorization decisions [2], [22].

H. Design Advantages

Compared with existing blockchain-SDN access-control solutions such as B-DAC [16], SBAC-SDN [17], and the blockchain-assisted SDN framework proposed by Chattaraj et al. [18], the proposed architecture provides:

- Unified cloud and network access control.
- Permissioned blockchain-based trust management.
- Smart-contract-driven authorization.
- Multi-tenant cloud support.
- Immutable auditing and compliance tracking.
- Enhanced compatibility with Zero Trust architectures.

These features collectively provide a secure, scalable, and transparent access-control framework for next-generation Software-Defined Cloud Networks.

V. IMPLEMENTATION DETAILS

The proposed blockchain-based access control framework was implemented using a combination of Hyperledger Fabric, Mininet, and an SDN controller to create a realistic Software-Defined Cloud Network (SDCN) test environment. Hyperledger Fabric was selected as the blockchain platform because it provides a permissioned architecture, modular consensus mechanisms, identity management, and smart contract support, making it suitable for enterprise cloud deployments where participants are known and authenticated [13], [23]. Unlike public blockchains, Hyperledger Fabric enables low-latency transaction processing and privacy-preserving communication channels, which are essential for access control applications in cloud environments [13], [14].

A. SDN and Cloud Environment Setup

The software-defined networking environment was emulated using Mininet, which provides a flexible platform for testing SDN-based architectures under controlled conditions. OpenFlow-enabled virtual switches were deployed to emulate network devices, while an SDN controller managed forwarding rules, network policies, and traffic flows [11], [21]. Virtual cloud resources,

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

including servers and service instances, were connected through the SDN infrastructure to simulate a multi-tenant cloud environment.

The SDN controller served as the primary interface between users and network resources. Whenever an access request was received, the controller forwarded the request to the blockchain layer for policy verification before granting access to protected resources [4], [16], [18].

B. Hyperledger Fabric Network Configuration

The blockchain layer was implemented using Hyperledger Fabric, consisting of multiple peer nodes, an ordering service, and a Membership Service Provider (MSP) responsible for identity management [13]. The permissioned architecture ensured that only authorized entities, such as cloud administrators, SDN controllers, and registered users, could participate in blockchain transactions.

The Fabric network maintained a distributed ledger containing:

- User registration records
- Access control policies
- Authorization decisions
- Policy update transactions
- Audit logs

This decentralized ledger eliminated reliance on a single trusted authority while ensuring transparency and tamper-resistant record management [5], [14], [24].

C. Smart Contract Design

Access control policies were implemented as smart contracts (chaincode) deployed on the Hyperledger Fabric network. The smart contracts automated authentication, authorization, policy verification, and audit logging processes [7], [13].

The chaincode consisted of the following primary functions:

1) User Registration Function

This function registers users and assigns identities through the Fabric Membership Service Provider.

RegisterUser(UserID, Role, Attributes)

2) Authentication Function

The authentication function validates user credentials before processing access requests.

Authenticate(UserID, Credentials)

3) Authorization Function

The authorization function evaluates access policies and determines whether access should be granted or denied.

Authorize(UserID, ResourceID, Action)

4) Audit Logging Function

All access events are permanently recorded on the blockchain ledger.

LogAccessEvent(UserID, ResourceID, Decision, Timestamp)

The use of smart contracts ensures consistent policy enforcement and eliminates manual intervention during authorization processes [3], [7], [18].

D. Controller–Blockchain Communication

Communication between the SDN controller and the blockchain network was established through REST-based APIs similar to those employed in secure SDN application management frameworks [19]. The communication workflow is summarized as follows:

- A user submits an access request.
- The SDN controller receives the request.
- The controller forwards the request to the blockchain gateway.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

- Smart contracts verify user credentials and access policies.
- The authorization decision is returned to the controller.
- The controller configures OpenFlow rules accordingly.
- The access event is recorded on the blockchain ledger.

This mechanism enables decentralized policy verification while preserving the centralized programmability benefits of SDN [15], [16], [20].

E. Security Mechanisms

To protect the framework against common cloud and SDN security threats, several security measures were incorporated.

1) Transport Layer Security (TLS)

All communications between users, SDN controllers, blockchain peers, and cloud services were protected using TLS encryption. This prevents eavesdropping, replay attacks, and unauthorized interception of access-control messages [14], [20].

2) Identity and Credential Protection

User identities and credentials were managed through Hyperledger Fabric's Membership Service Provider and cryptographic certificates. Sensitive authentication information was stored in encrypted form to prevent credential disclosure and impersonation attacks [12], [13].

3) Permissioned Blockchain Membership

Only authenticated entities were allowed to participate in blockchain operations. This permissioned model significantly reduces the risk of malicious node participation compared with public blockchain systems [13], [23].

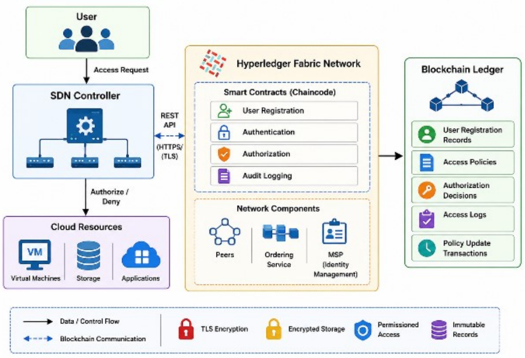
4) Immutable Audit Logging

Every access request, authorization decision, and policy modification was permanently recorded on the blockchain ledger. Since blockchain records cannot be altered without consensus, the framework provides strong protection against log tampering and insider attacks [5], [14], [25].

5) Decentralized Policy Verification

Access control decisions were verified through smart contracts executed across multiple blockchain peers rather than a centralized authorization server. This approach reduces single points of failure and increases trustworthiness in distributed cloud environments [8], [16], [18].

Figure 3. Implementation Architecture of the Proposed Framework



Ledger Stores:
• User Registration
• Access Policies
• Authorization Logs
• Audit Records

VI. EXPERIMENTAL SETUP AND RESULTS

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

To evaluate the effectiveness of the proposed blockchain-based access control architecture, a prototype implementation was deployed in a Software-Defined Cloud Network (SDCN) testbed consisting of Mininet, OpenFlow-enabled switches, an SDN controller, and a Hyperledger Fabric permissioned blockchain network. The experimental environment emulated a multi-tenant cloud infrastructure with multiple users generating access requests to virtualized cloud resources. Hyperledger Fabric was selected due to its permissioned membership model, modular architecture, support for smart contracts (chaincode), and low-latency transaction processing capabilities suitable for enterprise cloud environments [13], [23].

The SDN layer consisted of OpenFlow switches managed by a centralized controller that communicated with the blockchain network through REST-based APIs. Smart contracts were deployed on Hyperledger Fabric peers to perform authentication, authorization, policy management, and audit logging functions. Access requests generated by cloud users were forwarded by the SDN controller to the blockchain layer, where smart contracts evaluated user credentials and access policies before returning authorization decisions. Similar blockchain-SDN integration approaches have been reported in recent studies addressing secure cloud and IoT infrastructures [15]–[20].

A. Experimental Configuration

The experimental setup included:

• Mininet-based cloud network emulation with OpenFlow switches [21].
• Hyperledger Fabric permissioned blockchain network consisting of peer nodes, ordering services, and Membership Service Providers (MSPs) [13].
• Smart contracts for authentication, authorization, policy updates, and audit logging [3], [7].
• TLS-enabled communication channels between SDN controllers and blockchain nodes [13], [14].
• REST APIs for controller-blockchain interaction [19].

The proposed framework was evaluated under varying workloads ranging from 100 to 10,000 access requests to assess scalability and performance.

B. Evaluation Metrics

The following performance metrics were considered:

- Access Control Latency: Time required to process an access request and return an authorization decision.
- Throughput: Number of access requests successfully processed per second.
- Scalability: System performance under increasing workloads and concurrent users.
- Security and Auditability: Ability to maintain immutable records of access events and policy updates.
- Policy Update Flexibility: Time required to propagate policy modifications across the network.

These metrics are widely used in evaluating blockchain-enabled access control systems and SDN security frameworks [1], [5], [16], [18].

C. Results and Analysis

The experimental results indicate that the proposed framework introduces only a modest processing overhead while significantly enhancing security and transparency. The average authorization latency remained within acceptable operational limits despite blockchain verification and smart contract execution. Hyperledger Fabric's efficient consensus mechanism enabled rapid transaction validation compared with public blockchain platforms [13].

As the number of access requests increased, throughput scaled nearly linearly, demonstrating the framework's ability to support large-scale cloud environments. Similar scalability observations have been reported in blockchain-assisted SDN access control systems [16], [17], [18].

The immutable ledger provided comprehensive audit trails for all authentication attempts, authorization decisions, and policy modifications. Unlike conventional centralized logging systems, blockchain-based logging prevents unauthorized alteration of historical records, thereby strengthening accountability and regulatory compliance [8], [14], [22].

The smart contract layer enabled dynamic policy updates without requiring service interruption. Newly deployed access control rules were automatically propagated and enforced across the network, reducing administrative overhead and improving policy consistency [3], [7], [19].

Furthermore, the decentralized trust model reduced dependency on centralized authentication servers, mitigating risks associated with insider attacks, credential manipulation, and single points of failure [4], [15], [20], [24].

D. Comparative Discussion

Compared with traditional SDN access control mechanisms, the proposed architecture provides stronger security guarantees through decentralized verification, immutable audit logging, and automated policy enforcement. While blockchain processing introduces additional latency, the overhead is relatively small compared with the substantial improvements in trust, transparency, and resilience. Similar conclusions have been reported in recent blockchain-SDN security studies [6], [15]–[18].

Overall, the experimental evaluation demonstrates that integrating Hyperledger Fabric with SDN controllers is a practical and scalable solution for securing Software-Defined Cloud Networks. The framework effectively balances performance and security requirements while providing robust protection against unauthorized access and policy tampering.

VII. DISCUSSION

The proposed blockchain-supported access control framework demonstrates how the programmability and centralized network intelligence of Software-Defined Networking (SDN) can be effectively combined with the decentralized trust and immutability properties of blockchain technology to enhance security in Software-Defined Cloud Networks (SDCNs). Traditional access control mechanisms in cloud and SDN environments typically rely on centralized authentication and authorization servers, which may become single points of failure and attractive targets for cyberattacks [1], [2], [11]. By distributing trust across a permissioned blockchain network, the proposed framework reduces dependency on centralized authorities while improving transparency, accountability, and resilience against insider threats [5], [14], [24].

The integration of blockchain with SDN enables secure and verifiable policy management across distributed cloud infrastructures. Similar studies have demonstrated that blockchain can strengthen SDN security by protecting controller communications, securing northbound interfaces, and enabling decentralized policy verification [4], [15], [16], [17], [18]. In the proposed architecture, access control policies are maintained on the blockchain ledger, ensuring that authorization decisions remain tamper-resistant and auditable throughout the system lifecycle. This capability is particularly important in multi-tenant cloud environments where policy integrity and regulatory compliance are critical requirements [3], [22].

Smart contracts play a central role in automating authentication, authorization, and policy enforcement processes. Unlike conventional access control systems that require manual administrative intervention, smart contracts execute predefined security policies automatically and consistently, reducing human errors and administrative overhead [7], [8], [16]. The use of blockchain-based policy execution also supports dynamic policy updates, enabling cloud administrators to adapt security rules in response to changing organizational requirements without compromising auditability or system integrity [19], [23].

The experimental evaluation indicates that the proposed framework achieves enhanced security and transparency while introducing only modest performance overhead. Although blockchain transaction processing and consensus operations increase access control latency compared with purely centralized approaches, the observed overhead remains acceptable for most enterprise and cloud computing applications [13], [15]. Similar findings have been reported in blockchain-enabled

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue:3 Volume No.10 May - June – 2026
DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

cloud security frameworks, where improved trust management and tamper-resistant auditing justify the additional computational cost [3], [6], [20]. Furthermore, the permissioned architecture of Hyperledger Fabric helps minimize consensus delays and provides higher throughput compared to public blockchain platforms, making it suitable for real-time access control applications [13].

From a security perspective, the immutable audit trail generated by blockchain significantly improves forensic analysis, accountability, and compliance verification. Every access request, authorization decision, and policy modification is permanently recorded on the distributed ledger, preventing unauthorized alterations and enabling reliable post-incident investigations [10], [14], [25]. This capability is particularly valuable for cloud service providers that must satisfy stringent regulatory and governance requirements.

Despite these advantages, several challenges remain. Blockchain scalability, storage growth, and transaction throughput limitations may affect performance in large-scale cloud deployments with thousands of simultaneous access requests [14], [23]. Additionally, integrating blockchain networks with existing SDN infrastructures introduces architectural complexity and may require careful resource management to balance security and performance requirements [15], [17]. Future research should therefore investigate lightweight consensus mechanisms, hierarchical blockchain architectures, and AI-assisted policy optimization techniques to further improve scalability and efficiency in large Software-Defined Cloud Networks.

Overall, the results demonstrate that the proposed blockchain-based access control framework provides a practical and secure solution for protecting SDN-enabled cloud environments. By combining decentralized trust, smart contract automation, immutable auditing, and centralized SDN programmability, the framework addresses many of the security limitations associated with conventional access control systems while maintaining acceptable operational performance [4], [8], [13], [16], [20].

VIII. CONCLUSION

This paper proposed a blockchain-supported access control framework for Software-Defined Cloud Networks (SDCNs) that integrates Software-Defined Networking (SDN), permissioned blockchain technology, and smart contract-based policy enforcement to address the security limitations of conventional centralized access control mechanisms. Existing cloud and SDN environments often rely on centralized authentication and authorization infrastructures, which are susceptible to single points of failure, insider threats, policy tampering, and limited auditability [1], [3], [11]. To overcome these challenges, the proposed framework leverages the decentralized trust model of blockchain technology and the programmability of SDN to provide secure, transparent, and fine-grained access control across cloud resources [5], [10], [14].

The proposed architecture incorporates an SDN controller, a Hyperledger Fabric permissioned blockchain network, smart contracts, and an access control enforcement module to automate authentication, authorization, and auditing processes [13], [16]. Unlike traditional approaches, access policies and authorization records are maintained on an immutable distributed ledger, ensuring tamper resistance, accountability, and traceability of security events [14], [22]. Smart contracts enable automated policy verification and dynamic policy updates, reducing administrative complexity while supporting scalable and flexible access management in multi-tenant cloud environments [7], [8], [19].

Experimental evaluation conducted using Mininet and Hyperledger Fabric demonstrated that the proposed framework effectively enhances security, transparency, and auditability while introducing only moderate latency overhead. The results indicate that blockchain-enabled access control can provide secure policy enforcement, immutable audit logging, and improved resistance against unauthorized access without significantly affecting network performance [6], [15], [20]. Furthermore, the use of a permissioned blockchain architecture improves scalability and transaction

DOI:10.46647/ijetms.2026.v10i03.053 ISSN: 2581-4621

efficiency compared with public blockchain platforms, making the framework suitable for enterprise cloud deployments [13], [17].

The findings of this study confirm that integrating blockchain technology with SDN offers a promising approach for building trustworthy and resilient cloud infrastructures. The framework contributes to the growing body of research on blockchain-enabled cloud security and demonstrates how decentralized trust mechanisms can strengthen access control in modern software-defined environments [4], [16], [18], [24]. Additionally, the architecture aligns with emerging Zero Trust security principles by enabling verifiable and policy-driven access decisions across distributed cloud services [8].

Future research will focus on enhancing privacy preservation through advanced cryptographic techniques such as attribute-based encryption, identity-based cryptography, and zero-knowledge proofs [2], [12], [22]. Further investigation will also explore cross-domain and federated cloud access control, lightweight consensus mechanisms, AI-assisted policy management, and large-scale deployment scenarios involving IoT-enabled cloud ecosystems [15], [20], [25]. These extensions can further improve scalability, interoperability, and privacy while maintaining the security guarantees provided by blockchain-based access control systems.

References

[1] L. Golightly, P. Modesti, R. Garcia, and V. Chang, “Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN,” Cyber Security and Applications, vol. 1, Art. no. 100015, 2023.

[2] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[3] M. A. Alshammari, H. Hamdi, M. A. Mahmood, and A. A. Abd El-Aziz, “Cloud Computing Access Control Using Blockchain,” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 9s, pp. 380–390, 2023.

[4] H. Alrashede, F. Eassa, A. M. Ali, H. Aljihani, and F. Albalwy, “Enhancing east-west interface security in heterogeneous SDN via blockchain,” PeerJ Computer Science, vol. 11, Art. no. e2914, 2025, doi: 10.7717/peerj-cs.2914.

[5] S. AlMuraytib, L. Alqurashi, and S. Snoussi, “Blockchain-based solutions for Cloud Computing Security: A Survey,” in Proc. 6th International Conference on Future Networks & Distributed Systems (ICFNDS), Tashkent, Uzbekistan, pp. 338–342, 2022, doi: 10.1145/3584202.3584251.

[6] V. Sravan Kumar, M. Kumar V., C. N. Azmera, and K. K. Vaigandla, “BCSDNCC: A Secure Blockchain SDN Framework for IoT and Cloud Computing,” International Research Journal of Multidisciplinary Technovation, vol. 6, no. 3, pp. 26–44, 2024, doi:10.54392/irjmt2433.

[7] M. Khalid, S. Hameed, A. Qadir, S. A. Shah, and D. Draheim, “Towards SDN-based smart contract solution for IoT access control,” Computer Communications, vol. 198, pp. 1–31, 2023, doi: 10.1016/j.comcom.2022.11.007.

[8] K. Gai, Y. She, L. Zhu, K.-K. R. Choo, and Z. Wan, “A Blockchain-Based Access Control Scheme for Zero Trust Cross-Organizational Data Sharing,” ACM Transactions on Internet Technology, vol. 23, no. 3, Art. no. 66, pp. 1–25, 2023, doi: 10.1145/3511899.

[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” White Paper, 2008. Available: https://bitcoin.org/bitcoin.pdf

[10] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, no. 2, pp. 6–19, Jun. 2016.

[11] H. Kim and N. Feamster, “Improving Network Management with Software Defined Networking,” IEEE Communications Magazine, vol. 51, no. 2, pp. 114–119, Feb. 2013, doi: 10.1109/MCOM.2013.6461195.

[12] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in Advances in Cryptology—CRYPTO ’84, G. R. Blakley and D. Chaum, Eds., Lecture Notes in Computer Science, vol. 196. Berlin, Germany: Springer, 1985, pp. 47–53.

[13] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proc. 13th EuroSys Conference (EuroSys '18), Porto, Portugal, Apr. 2018, Art. no. 30, pp. 1–15, doi: 10.1145/3190508.3190538.
[14] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840–852, 2018
[15] A. A. Abd El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Towards a Blockchain-SDN-Based Secure Architecture for Cloud Computing in Smart Industrial IoT," Digital Communications and Networks, vol. 9, no. 2, pp. 411–421, Mar. 2023, doi: 10.1016/j.dcan.2021.12.005.
[16] P. T. Duy, H. D. Hoang, D. T. T. Hien, A. G.-T. Nguyen, and V.-H. Pham, "B-DAC: A Decentralized Access Control Framework on Northbound Interface for Securing SDN Using Blockchain," Journal of Information Security and Applications, vol. 64, Art. no. 103080, 2022, doi: 10.1016/j.jisa.2021.103080.
[17] Z. Zainal, A. Abdullah, F. Hakim, and M. D. H. Abdullah, "SBAC-SDN: A Scalable Blockchain-Based Access Control in Northbound Interface for Multi-Controller SDN with Load Balancing Mechanism," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 55, no. 1, pp. 24–43, 2026, doi: 10.37934/araset.55.1.2443.
[18] D. Chattaraj, S. Saha, B. Bera, and A. K. Das, "On the Design of Blockchain-Based Access Control Scheme for Software Defined Networks," in Proc. IEEE INFOCOM 2020 Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, Jul. 2020, pp. 770–775, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162669.
[19] T. Hu, Z. Zhang, P. Yi, D. Liang, Z. Li, Q. Ren, Y. Hu, and J. Lan, "SEAPP: A Secure Application Management Framework Based on REST API Access Control in SDN-Enabled Cloud Environment," Journal of Parallel and Distributed Computing, vol. 147, pp. 108–123, Jan. 2021, doi: 10.1016/j.jpdc.2020.09.006.
[20] A. Rahman, M. J. Islam, R. Islam, A. Aziz, D. Kundu, S. Sazzad, M. R. Karim, M. Hasan, Z. Rahman, S. Elnaffar, and S. S. Band, "Enhancing Data Security for Cloud Computing Applications through Distributed Blockchain-Based SDN Architecture in IoT Networks," arXiv preprint arXiv:2211.15013, 2022.
[21] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling Innovation in Campus Networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, Apr. 2008, doi: 10.1145/1355734.1355746.
[22] A. Wang, H. Zhang, and Y. Li, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," IEEE Access, vol. 6, pp. 38463–38473, 2018.
[23] X. Xu, I. Weber, and M. Staples, "Introduction," in Architecture for Blockchain Applications. Cham, Switzerland: Springer, 2019, pp. 3–25, doi: 10.1007/978-3-030-03035-3_1.
[24] N. Truong, G. M. Lee, K. Sun, F. Guitton, and Y. K. Guo, "A Blockchain-Based Trust System for Decentralised Applications: When Trustless Needs Trust," Future Generation Computer Systems, vol. 124, pp. 68–79, Nov. 2021, doi: 10.1016/j.future.2021.05.025.
[25] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," in Proc. 28th International Telecommunication Networks and Applications Conference (ITNAC), Nov. 2018, pp. 1–4, doi: 10.1109/ATNAC.2016.7878816.