The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 11 | November 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

A review on Block chain-Based Authentication Frameworks for Cloud Network Security

Neha[1], Neha gupta[2], Shehbaaz Singh Brar[3]

[1]Assistant Professor(IT),GNDEC, Ludhiana ,Punjab,India

[2]Assistant Professor(CA), GNDEC ,Ludhiana, Punjab,India

[3]Assistant Professor(ME), GNDEC ,Ludhiana, Punjab,India

Email: ngarg2045@gmail.com[1], guptan422@gmail.com[2], shehbaazsbrar@gmail.com[3]

DOI : https://doi.org/10.5281/zenodo.17922070

ARTICLE DETAILS

Research Paper

Accepted: 21-11-2025

Published: 10-12-2025

Keywords:

Blockchain; Authentication; Cloud Security; Decentralized Identity; Access Control; Smart Contracts; Multi-Factor Authentication; Trust Management

ABSTRACT

Cloud computing has revolutionized the role of data and service management of organizations but it poses significant security risks of authentication and access control. Classical centralized identity management and authentication systems are characterized by failure and trust points hence exposed to attacks and unavailability. The blockchain technology provides an alternative to authentication frameworks that is decentralized, proves tamper-evident, and offers a distributed trust, transparency, and strong security. The aim of this paper is to review the authenticity models of blockchain in cloud network security at an academic level of SCI/SCOPUS. We conduct a survey of the recent quality research on the topic of blockchain as an enhancing feature of authentication in clouds and multi-clouds. The paper explains the reasons why blockchain (immutability, decentralization, and increased trust) should be in place and explores different suggested frameworks, such as decentralized identity management systems, blockchain-based single sign-on systems, blockchain-based access control based on smart contracts, and blockchain-based public key infrastructures. The important characteristic of representative frameworks that we compare include

the integration of multi-factor authentication, scalability, performance overhead, and interoperability, which we discuss in a special table. Based on the information gathered in the literature, we subsequently offer a conceptual blockchain-based authentication system specific to cloud network security that integrates the best practices such as consortium blockchains, adaptive multi-factor, and smart-contract governance. To demonstrate the secure access flows based on the use of blockchain as a trust anchor, a case study architecture is provided. Lastly, we also address open challenges (including scalability, privacy, and standardization) and the future of this quickly changing field. The results show that blockchain-based authentication has a significant potential to improve cloud safety by increasing centralized vulnerabilities and granting verifiable and distributed trust of identities, but viable implementation factors (e.g., performance and integration with existing systems) need further investigation

Introduction

The security of authentication in cloud networks is a prerequisite issue since more organizations depend on cloud services. Cloud environments are highly distributed, multi-tenant and frequently cross-service provider which makes traditional identity and access management (IAM) difficult. In traditional cloud environments, user access and authentication are normally managed by centrally located identity providers or authentication server (e.g. single sign-on server or directory service). This centralized system is also known to have some widely recognized disadvantages: such a model introduces single points of failure and valuable targets to attackers, and it asks users and organizations to trust the security of the identity provider entirely. Well-known cases have demonstrated that the loss of an authentication server or its failure can cause the extensive data leakage or loss of service functioning in the cloud ecosystem (Punia et al., 2024). In addition, centralized IAM solutions are not always that transparent - users and clients must have faith that the authentication logs and mechanisms are correct and are unable to check them easily on their own (Pham et al., 2025). These restrictions allow studying decentralized ways of cloud authentication.

The adoption of blockchain technology has become an attractive solution to these issues since it will decentralize trust and stimulate security during authentication (Kumar et al., 2019; Pham et al., 2025). A

blockchain is a distributed registry that is run by a network of nodes instead of one authority, thus it is resistant to a single-point failure and manipulation. After the data (authentication event or user credential) is stored on the blockchain, it becomes highly inaccessible to modify or delete because of cryptographic connectivity of blocks - this will create an unchangeable audit trail of identity and access events (Novo, 2018). This immutability and transparency can enhance the accountability of authentication systems to a considerable degree (Pham et al., 2025). To give an example, making the logins or access grant recordings on a blockchain ledger allows auditing them by all parties involved to prevent malicious activity and facilitate compliance audit. Also, the consensus mechanisms of blockchain decentralize the power of verification among a number of nodes; therefore, a compromised server cannot obtain an identity verification or unlawfully provide access to the system without being identified (Jamal et al., 2019). With such properties, scientists and professionals have begun to develop blockchain-based authentication system to enhance cloud network security.

This field has a number of research directions that have been intersecting. One of these directions is based on decentralized identity management (DIM), frequently using blockchain to support self-sovereign identity - in which users can maintain their own digital identities without depending on any provider (Muhle et al., 2018). The other approach is to apply smart contracts (programmable logic on blockchains) to enforce an authentication and authorization policy that automatically enforces access rules transparently but in an unalterable way (Alatawi, 2025). There are also specialized domain frameworks such as the Internet of Things (IoT), edge computing, and healthcare where blockchain-based authentication can be applied to secure device interactions with cloud services and user interactions with cloud service providers (Novo, 2018; Al Hwaitat et al., 2023). They are frequently combined with other methods: some of these frameworks are based on multi-factor authentication (MFA) and biometrics with blockchain to provide greater confidence in user identity (Zhao et al., 2023), and others use blockchain as a foundation of a public key infrastructure (PKI) - managing digital certificates and revocations in a decentralized manner (Saleem et al., 2022). The fact that there are a variety of approaches explains the adaptability of blockchain to various areas of cloud security.

The paper gives an in-depth research of the state-of-the-art in blockchain-based authentication systems in an effort to secure cloud networks. We scan the literature of the best quality published within the recent years (from 2019-2025, in particular) to determine the major frameworks, patterns of design, advantages, and issues. Once the requisite background has been discussed, we tabulate and talk about the significant frameworks in the academic and industry perspectives. Then we give a comparative analysis of

representative solutions (in table format) in order to see their characteristics and differences. Through the inferential knowledge acquired, a conceptual approach is presented, which combines the best practices identified in the literature such as decentralized identity management, implementation of consortium blockchain, adaptive multi-factor authentication, and implementation of smart contracts to govern access to cloud networks. We also provide an example figure showing the way such a framework can be used in a cloud environment. The paper is finally concluded with the discussions on the open challenges (such as scalability and privacy) and the directions of research, as the field keeps developing at the high pace.

Background and Motivation

Cloud Authentication Challenges and Threats

The security of authentication in cloud networks is a prerequisite issue since more organizations depend on cloud services. Cloud environments are highly distributed, multi-tenant and frequently cross-service provider which makes traditional identity and access management (IAM) difficult. In traditional cloud environments, user access and authentication are normally managed by centrally located identity providers or authentication server (e.g. single sign-on server or directory service). This centralized system is also known to have some widely recognized disadvantages: such a model introduces single points of failure and valuable targets to attackers, and it asks users and organizations to trust the security of the identity provider entirely[1][2]. Well-known cases have demonstrated that the loss of an authentication server or its failure can cause the extensive data leakage or loss of service functioning in the cloud ecosystem (Punia et al., 2024). In addition, centralized IAM solutions are not always that transparent - users and clients must have faith that the authentication logs and mechanisms are correct and are unable to check them easily on their own (Pham et al., 2025). These restrictions allow studying decentralized ways of cloud authentication.

The adoption of blockchain technology has become an attractive solution to these issues since it will decentralize trust and stimulate security during authentication (Kumar et al., 2019; Pham et al., 2025). A blockchain is a distributed registry that is run by a network of nodes instead of one authority, thus it is resistant to a single-point failure and manipulation. After the data (authentication event or user credential) is stored on the blockchain, it becomes highly inaccessible to modify or delete because of cryptographic connectivity of blocks - this will create an unchangeable audit trail of identity and access events (Novo, 2018). This immutability and transparency can enhance the accountability of authentication systems to a considerable degree (Pham et al., 2025). To give an example, making the

logins or access grant recordings on a blockchain ledger allows auditing them by all parties involved to prevent malicious activity and facilitate compliance audit. Also, the consensus mechanisms of blockchain decentralize the power of verification among a number of nodes; therefore, a compromised server cannot obtain an identity verification or unlawfully provide access to the system without being identified (Jamal et al., 2019). With such properties, scientists and professionals have begun to develop blockchain-based authentication system to enhance cloud network security.

This field has a number of research directions that have been intersecting. One of these directions is based on decentralized identity management (DIM), frequently using blockchain to support self-sovereign identity - in which users can maintain their own digital identities without depending on any provider (Muhle et al., 2018). The other approach is to apply smart contracts (programmable logic on blockchains) to enforce an authentication and authorization policy that automatically enforces access rules transparently but in an unalterable way (Alatawi, 2025). There are also specialized domain frameworks such as the Internet of Things (IoT), edge computing, and healthcare where blockchain-based authentication can be applied to secure device interactions with cloud services and user interactions with cloud service providers (Novo, 2018; Al Hwaitat et al., 2023). They are frequently combined with other methods: some of these frameworks are based on multi-factor authentication (MFA) and biometrics with blockchain to provide greater confidence in user identity (Zhao et al., 2023), and others use blockchain as a foundation of a public key infrastructure (PKI) - managing digital certificates and revocations in a decentralized manner (Saleem et al., 2022). The fact that there are a variety of approaches explains the adaptability of blockchain to various areas of cloud security.

The paper gives an in-depth research of the state-of-the-art in blockchain-based authentication systems in an effort to secure cloud networks. We scan the literature of the best quality published within the recent years (from 2019-2025, in particular) to determine the major frameworks, patterns of design, advantages, and issues. Once the requisite background has been discussed, we tabulate and talk about the significant frameworks in the academic and industry perspectives. Then we give a comparative analysis of representative solutions (in table format) in order to see their characteristics and differences. Through the inferential knowledge acquired, a conceptual approach is presented, which combines the best practices identified in the literature such as decentralized identity management, implementation of consortium blockchain, adaptive multi-factor authentication, and implementation of smart contracts to govern access to cloud networks. We also provide an example figure showing the way such a framework can be used in

a cloud environment. The paper is finally concluded with the discussions on the open challenges (such as scalability and privacy) and the directions of research, as the field keeps developing at the high pace.

Blockchain-Based Authentication Frameworks: State of the Art

Authentication infrastructure based on blockchains to secure cloud environments can be generally divided according to their priorities and design methodology. Some of the categories with examples are discussed below and how each type of framework improves security and the trade-offs, are summarized.

Self-Sovereign Authentication and Decentralized Identity.

Decentralized identity management is one distinguished category and tends to converge with the idea of Self-Sovereign Identity (SSI). Users in SSI systems are in control of their identity information, which is usually blockchain-based, instead of having user identities and credentials stored and authenticated by a central IdP. They are able to provide credentials (digitally signed by the issuers, such as governments or organizations) that can be verified by the verifiers against blockchain records as legitimate.

As an illustration, Mostafa et al. (2025) suggest a decentralized model of IDM in cloud computing with ethereum smart contract and auto provisioning methods to enhance the scales and security. Within their system, the users are backed by a blockchain profile and are able to access several cloud services via a single sign-on (SSO) (Mostafa et al., 2025). The Ethereum blockchain contains smart contracts holding and verifying user roles and permissions (in accordance with a Role-based Access Control model). The primary characteristics of such a system are the ability to allow multifactor authentication (to enhance the verification of the user of the control over the identity) and the delegated proof-of-stake (DPoS) consensus mechanism to accelerate transactions within the private blockchain network (Mostafa et al., 2025). What emerges is an identity system in which the trust is distributed - no cloud provider has the monopoly on identification records, and any identity-related action (such as removing access privileges of a user) would be logged on the blockchain ledger to make it transparent.

The other example is the use of Decentralized Identifiers (DID) as a W3C standard. A DID describes an entity (person, device, etc.) that is identified on a blockchain that is accompanied by public keys and possibly endpoints to access additional credentials. Such networks of decentralized identity have been deployed in blockchain endeavors such as Sovrin/Hyperledger Indy. Within such frameworks, a cloud service outcomes that a user is to be authenticated can prove that they have control over their DID (typically by cryptographic challenge), and can retrieve verifiable credentials (e.g., Alice is an employee

of Company X with role Y) on the blockchain or a decentralized storage, and verify their signatures using blockchain trust anchors (Muhle et al., 2018). The blockchain basically substitutes the central certificate authority/identity provider since it is the publicly accessible registry of identity attestations and revocations.

The security benefit is obvious: customers are not dependent any longer on dozens of cloud functions which store their passwords or personal data. Rather, the identity information of the user lies in their hands (usually saved in an identity wallet application) and data sharing is voluntary and limited. On the side of the cloud provider, authentication is reduced to checking a blockchain anchored signature or credential, which is naturally more difficult to counterfeit or modify than conventional tokens or passwords. The credentials may be revoked (e.g. an employee leaving a company) by simply writing a revocation record to the blockchain, and immediately informing the entire verifier network around the world. Nonetheless, the systems are only useful in a broadly adopted and standardised form and something to defend user privacy (because inscribing identity data to an immutable ledger may violate privacy laws unless done with great care, e.g., by posting non-sensitive cryptographic proofs or hashes on-chain only).

Frameworks of blockchain-based access control and authorization.

Whereas identity framework determine who the user or entity is, access control frameworks determine what the authenticated entity can do. Blockchain has also been exploited by various scholars to implement distributed access control solutions to internet of things and cloud networks. Policy analysis and decision documentation in these systems is carried out on the blockchain, lowering the probability of policy manipulation and giving a single perspective of access permissions.

One of the most striking plans by Yu et al. (2023) is combined authentication and authorization of distributed mobile cloud services. They suggest a blockchain-oriented system, in which a user registers once with any one of the cloud providers (SP) in a group of cloud providers and could then use the same credential to access services of other providers in the group (Yu et al., 2023). This is similar to a federated identity system except that there is no central federation state, rather the blockchain (here executed through Hyperledger Fabric) takes the responsibility of maintaining the identity of users to their permissions in each service. Smart contracts support dynamic updates on access permissions: as the access level of one of the users in one of the services is changed, the update (with the appropriate authorization) is added to a blockchain and is visible to all other providers in real-time (Yu et al., 2023).

Each user only requires a single blockchain transaction to capture his/her access rights with all providers, which is cost-effective with regards to storage on the chain. In this scheme, the individual provider can do away with authenticating the user individually, or with verifying with a central SSO server; the shared ledger is consulted. Security analysis Yu et al. performed revealed that the scheme is resistant to impersonation and man-in-the-middle attacks using a random oracle model, and performance analysis demonstrated that the scheme incurs only a small overhead over traditional multi-server authentication (Yu et al., 2023). Simply, it is a single sign-on of cloud federations with decentralization and trust is not established through a bilateral agreement but instead through the blockchain.

In another example, Alatawi (2025) proposed a framework based on blockchain-based smart contracts able to employ fine-grained authorization to cloud security. Within this model, users (authenticate their requests with a multi-factor approach) send their requests to a blockchain smart contract that implements authorization policies before accessing or rejecting cloud resources (Alatawi, 2025). Since the smart contract allows only valid and pre-defined operations, a large number of attacks, such as privilege escalation or unauthorized modification of data, are prevented - any attempt that does not match the logic of the contract will just fail. The application of Alatawi to Ethereum showed that such a system could be very secure (almost zero attempts of unauthorized access were recorded during tests) with the cost of additional latency under heavy load caused by blockchain transaction processing[3][4]. It is also important to note the implementation of Multi-Factor Authentication (MFA) in this system: the user will have to verify several factors (password, OTP, biometric, and so on) and the blockchain contract also authenticates the presence of the proof of each of them, and it will be much more difficult to impersonate the identity in the case of one of the factors (such as a password) being stolen (Alatawi, 2025).

IoT-cloud ecosystems have also been investigated in the field of access control frameworks based on blockchain. Indicatively, Novo (2018) designed one of the first architectures known as the Blockchain Meets IoT, which practically relies on a public Ethereum blockchain to control the access rights of devices of the IoT. On the blockchain, every IoT device on the cloud platform is identity-based and whenever a device requires to access or publish data, it is required to provide a transaction signed with its own key to demonstrate its identity and authorization (Novo, 2018). Smart contracts are utilized to control access control lists and roles, without the central brokerage of a centralized controller. This pattern proved to be a way to spread trust and prevent individual failure, but it brought up the question of the cost of blockchain transactions and throughput of large systems of integration (problems that newer designs usually solve with permissioned or scalable blockchains).

Adaptive Multi-Factor Schemes and Context-Aware Schemes.

Some frameworks add adaptivity and context-awareness to the simple concept of blockchain-based auth. An example is Zhao et al. (2023), who created an authentication scheme whose selection of multi-factors is adaptive. Their implementation style involves the smart selection of which factors to demand of the user by the authentication system, depending on the circumstances (e.g. the device in use, its location, the riskiness of the request) - and this selection policy is implemented using blockchain (Zhao et al., 2023). The plan will consist of a blockchain-based authentication system and a set of custom consensus (called LRaft) optimized to reach quick consensus among authentication nodes (Zhao et al., 2023). With the multi-factor evaluation being run on-chain, the framework means that a malicious actor that somehow compromises one of the factors cannot evade the need to have other factors, as the combination of the factors required is determined and checked by the blockchain nodes jointly. The findings indicate improved resistance to frequent attacks (brute force, replay, etc.) and zero failure point in the auth flow (Zhao et al., 2023). Such adaptive methods emphasize how blockchain can be used not only to allow identity to be confirmed in a static manner, but also dynamically adapt security requirements in a trusted manner. Frequently, the inclusion of adaptive authentication in a traditional system implies accepting a central risk engine - but with a blockchain, the risk assessment policies may be written in an open contract that everyone is convinced of, making it impossible to subvert or err in policy enforcement.

One more solution with innovative schemes is presented by Jin and Omote (2024): transferable authentication in cloud-IoT. They suggest a very effective blockchain-based authentication system in which a user may provide a one-time authentication permission to another party (Jin and Omote, 2024). As an illustration, a user can once authorize a service or agent to access a resource on behalf of the user. The algorithm relies on smart contracts as a single-use verifier: the user will create a one-time key (an OTP with a proof-of-work token by using Hashcash) and sign it to the blockchain. The respective agent may then utilize that key to validate via the smart contract which will accept it once and invalidate it after that (Jin and Omote, 2024). This means that the key cannot be reused or abused more broadly than intended - a feature that is very useful in delegated access in cloud services (such as providing a temporary maintenance service temporary access to a virtual machine instance). The design by Jin and Omote does so without significant public-key operations or zero-knowledge proofs, and uses hash functions and the statefulness of the blockchain, making the computational overhead low. It is an excellent demonstration of how blockchain can help facilitate new capabilities in authentication (such as controlled delegation and one-time credentials) which is cumbersome to secure in centralised systems.

Certificates and Certificate Management Based on blockchain-Enhanced Public Key Infrastructure (PKI).

Many authentication systems (ex: TLS certificates to authenticate the server, or SSH keys to authenticate a cloud VM) are based on public key cryptography. Traditional PKI has centralized certificate authorities (CA) which issue and revoke certificates. Blockchain systems have been suggested to decentralize this factor also, hence enhancing network authentication in cloud services (which frequently uses PKI to secure connection and code).

Proof Chain is an X.509-based PKI framework based on blockchain, presented by Saleem et al. (2022). In Proof Chain, smart contracts on a blockchain perform several roles of certificate authorities (or supplement), and include decentralized trust to issue, validate, and revoke certificates (Saleem et al., 2022). The issuance of every certificate is recorded on the blockchain forming a transparent registry - any client can always check the blockchain to find the fingerprint and validity of the certificate of a server, instead of checking one that could be compromised central CA or certificate transparency log. Revocations are also managed by merely changing the status of a certificate on-chain and are instantly apparent to all verifiers (Saleem et al., 2022). The framework can interoperate with an existing TLS/SSL infrastructure, i.e. it can be integrated without entirely reinventing the certificate format (it is X.509-compatible). In the case of a cloud network, this implies that internal services or microservices have the ability to verify the certificates of each other using the blockchain, which lessens the chances of man-in-the-middle attacks using forged certificates. It also alleviates such concerns as rogue CAs: no CA can quietly issue an evil certificate since the blockchain registry will reveal the issuance to everyone, and it may take the agreement of multiple nodes (which might belong to different organizations) to accept a new certificate. Decentralized blockchain-PKI trust model eliminates the archetypal situation where a compromised root CA is used to impersonate individuals on large scale levels. Naturally, performance and scalability should be handled - the read or write of the blockchain will add latency to local certificate store. Permissioned blockchains or consortium networks are often utilized in ProofChain and other initiatives to make the throughput and latency reasonable to be used in the real-world (Saleem et al., 2022). This is a trade-off, a permissioned blockchain (e.g., managed by a group of cloud providers or enterprises) may be much faster to achieve consensus than a public one, but at slightly lower levels of decentralization (it is still much better than a single power).

Zero Trust Architectures and Trust Management.

In addition to direct authentication and authorization, not all blockchain are used in a zero trust architecture, some of them are used to provide continuous trust assessment. According to Zero Trust Architecture (ZTA), all access requests must be checked and validated again, and horizontal movement within a network must not be inherently relied upon. The logging feature of blockchain is a natural complement to this, in that it is capable of keeping a live record of trust scores, device conditions, or flags of anomalies that are shared between an ecosystem.

As an example, Jamal et al. (2019) proposed a blockchain-based solution to introduce a zero trust organization. They paid attention to dynamic trust management when the trustworthiness of each entity is measured regularly (via analysis of behavior, health checks of device, etc.) and stored on a blockchain (Jamal et al., 2019). These trust levels, stored in blockchain are then taken into account to make authentication decisions. Due to the distributed trust ledger being append-only, an insider can no longer tamper with their trust score in the background and every network device/user has an agreed on perspective of the most recent trust status of others. In essence, the blockchain is a distributed risk assessment database that is an input of authentication policies. To take a specific example, when a specific server has been identified to have abnormal activity and its trust score decreases (as reported by an intrusion detection system to the chain), other parts can automatically demand extra authentication factors of the server requests or restrict access to it, until the problem is resolved and the score increases (Jamal et al., 2019). This type of dynamically, data-driven authentication control is extremely difficult to organize in a conventional configuration, yet a blockchain has offered a source of one truth of trust metrics within a zero trust model.

On the same note, other cloud/edge trust systems apply blockchain to scale device identities and credentials. Other proposals store the identities of IoT devices on blockchain and perform on-chain transactions as a way to certify the integrity of firmware of a device or its security posture. Once such devices are linked to the cloud services, they can be authenticated by the cloud querying the blockchain to determine their latest attestation status as opposed to a fixed credential (Wang et al., 2021). The cloud network therefore continuously authenticates, not only the user, but also the state of the device - a valuable feature in the case of IoT-intensive cloud systems.

Table: Comparison of Selected Frameworks

To better visualize the landscape, **Table 1** provides a comparison of several representative blockchain-based authentication frameworks, highlighting their blockchain platform, key features, and the context

they are designed for. This comparison underscores how different frameworks prioritize certain aspects (e.g., performance vs. decentralization, general-purpose vs. domain-specific designs).

Framework & Source	Blockchain Platform	Key Features	Use Case / Domain
Deep et al. (2019) – Cloud DB Auth Protocol *[Sensors]*	Public Ethereum (permissionless)	*Peer-to-peer* user authentication for cloud databases; single private key for multi-provider access; on-chain credential verification	General Cloud (Database access)
Novo (2018) – IoT Access Management *[IEEE IoT J]*	Public Ethereum (smart contracts)	Decentralized IoT device authentication; blockchain stores device permissions; no central broker; role-based access via contracts	IoT-Cloud Integration
Jamal et al. (2019) – Zero Trust Framework	Consortium Blockchain	Continuous trust scoring on-chain; dynamic access decisions based on on-chain trust metrics; eliminates implicit trust zones	Enterprise Zero Trust Networks
Yu et al. (2023) – Multi-Cloud Auth Scheme *[Sensors]*	Hyperledger Fabric (permissioned)	Single sign-on across multiple cloud providers; one blockchain transaction encapsulates a user's rights on all services; dynamic permission updates via chaincode	Federated Cloud Services (Mobile Cloud)
Al Hwaitat et al. (2023) – IoT Network Auth *[Electronics]*	Private Ethereum network	Authentication for resource-constrained IoT; lightweight consensus for efficiency; stores device IDs and uses blockchain as trust anchor between fog, cloud, and devices	Secure IoT networks (smart homes, etc.)
Zhao et al. (2023) – Adaptive MFA Scheme *[Mobile Info. Sys.]*	Consortium (Raft-based)	Adaptive multi-factor authentication (context-aware factor selection); custom LRaft consensus for fast auth decisions; robust against single-factor compromise	Mobile and Dynamic Cloud Applications

Framework & Source	Blockchain Platform	Key Features	Use Case / Domain
Jin & Omote (2024) – One-Time Auth Scheme *[PLoS One]*	Public Ethereum (Goerli testnet)	One-time authentication tokens with Hashcash PoW; transferable auth delegation via smart contract; no need for ZKP or heavy crypto (uses hashes)	Delegated IoT/Cloud service access
Alatawi (2025) – Smart Contract Auth *[Electronics]*	Private Ethereum network	MFA integrated (password, OTP, biometrics) into blockchain auth flow; fine-grained access control by smart contracts; extensive security metrics evaluation (attacks logged on-chain)	Cloud User Authentication & Authorization
Mostafa et al. (2025) – Decentralized IDM *[Int. J. Int. Sys.]*	Ethereum (permissioned DPoS)	Self-sovereign identity for cloud users; supports SSO and RBAC via smart contracts; uses DPoS + machine learning for fraud detection (trustworthy transactions)	Cloud Identity Management (Enterprise)
Saleem et al. (2022) – ProofChain PKI *[Comp. Networks]*	Multi-Chain/Custom (consortium)	Blockchain-based certificate issuance and revocation; X.509-compatible for easy integration; decentralized trust (no single CA); real-time revocation checks on-chain	Global PKI for Cloud & Internet

Table 1: Comparison of selected blockchain-based authentication and identity frameworks. Each framework leverages blockchain properties to achieve improvements in trust, security, or flexibility for cloud network authentication. (Abbreviations: MFA = Multi-Factor Authentication, SSO = Single Sign-On, RBAC = Role-Based Access Control, PKI = Public Key Infrastructure, CA = Certificate Authority, DPoS = Delegated Proof of Stake, ZKP = Zero-Knowledge Proof.)

The above table and discussions illustrate the rich design space. Some frameworks opt for permissionless blockchains to maximize decentralization (e.g., using Ethereum mainnet for trustlessness), but they must handle performance bottlenecks and cost (transaction fees). Others choose permissioned or consortium chains to strike a balance, achieving higher throughput and faster consensus at the cost of involving a trusted group (like known organizations running the nodes). The appropriate choice often depends on the deployment scenario: **enterprise clouds may favor consortium chains** operated by a coalition of cloud

providers or stakeholders, whereas open internet use-cases might lean towards public chains or at least widely decentralized networks to avoid any single point of trust.

Proposed Integrated Framework for Cloud Network Authentication

Our analysis of the current solutions and strengths of them led us to present a suggested holistic model of blockchain-based cloud authentication that would ensure the high-security level demanded by the contemporary cloud network and be feasible at the same time.

Framework Overview: This framework proposes a consortium blockchain operated by key stakeholders (e.g., cloud providers, identity authorities, maybe large clients) which acts as a universal trust anchor to identity and access transactions. Figure 1 shows the conceptual architecture and it is based on reference designs in literature. The system is made up of the following:

Decentralized Identity Layer: The system is characterised by a Decentralized Identifier on the blockchain, which represents each user or device in the cloud system. They have a public/private key pair; the public key (or a hash of it) is stored on-chain with their DID, and can be supplemented by verifiable credentials (attributes such as roles, certifications) that are issued by trusted entities (e.g. an employer or a device maker). Identity creation and updates (such as the addition of a new attribute or the revocation of one) are performed via blockchain transactions, so multi-party consensus is required (to ensure that a rogue or erroneous identity update can be detected by others).

Authentication Process: The user (or device) to access a cloud service presents a cryptographic identity evidence in order to log in or demand entry. As an example, the user may use the signature of a challenge nonce through signing by using their private key (demonstrating possession of the key of the DID). This evidence, with additional necessary second components (e.g., one-time code, biometric attestation) is posted to the blockchain network of the consortium (through an API gateway). A smart contract stored on the blockchain authenticates the signature with the public key of the user stored and authenticates second-factor tokens. Since this contract is performed through several blockchain nodes, the outcome is reached through consensus. When the authentication passes, a log record is made on-chain and temporary authentication token (possibly a signed JWT or reference to an on-chain session record) is sent back to the user to be used in accessing services. In case invalid, the attempt to log in is recorded (deterrent to re trying, as it becomes part of an audit trail that admins can look at, which will forever be visible and impossible to alter).

Access Control using Smart Contracts: An authenticated user may only make requests on a cloud resource (e.g., access a database, invoke an API), and in that case, the access proxy of the resource will consult the smart contract in the blockchain to issue authorization. A smart contract encodes the access policy (of that resource or service) - e.g. permission to some roles or some attributes. The proxy uses the DID of the user and the action they are requesting in a query (transact or call) with the contract. This contract will then verify: (a) that the user authentication token/session is recent and valid (to prevent reuse of old sessions), and (b) the user roles/attributes satisfy the policy of that action. Upon approval, the contract generates an event (or sends an approved back) which the proxy relies on to permit the action. All this decision will be logged in, to form an unaltered access record.

Adaptive Security and Trust Management: The framework will allow incorporating risk-based authentication, such as providing a trust score of each identity on the blockchain. One can update this score by observing services, e.g. an anomaly detector that is based on machine learning can issue an update when the behavior of a user appears suspicious or when a device may be broken into (Mostafa et al., 2025 works with an AI to detect fraud during transactions). The smart contracts can be coded so that requirements change according to the level of trust: e.g. when a user has a low score on trust, the contract may require MFA on all access or tie up the account until a human can verify per the account. These are on-chain trust and risk indicators that are universal across all the cloud services in the consortium.

Privacy-Saving Solutions: To prevent revealing sensitive data to the blockchain, our architecture receives cryptographic tokens and hashes. The blockchain does not store personal data in plaintext, but only the verification data (public keys, attribute commitments, and so on). Such methods as zero-knowledge proofs may be utilized in case, say, we need to prove that a person is over 18 years old or has a specific clearance but not the actual value - the verification of the proof is possible with the help of a smart contract and the public key of an issuer, which is stored in the chain. Also, the consortium blockchain can impose an access control on identity information: only authorized actors (the user or need-to-know services) may access specific information, which can be done through encrypted information stored in-chain with keys delivered to authorized parties.

Workflow Summary: An administrator Alice wishes to log in to the cloud management console of her company. Alice contains a DID in the consortium blockchain with attributes that identify her as an admin. Alice authenticates using her identity wallet by signing a challenge and her OTP. This is validated by the blockchain nodes through the identity contract (multipolar verified) and is recorded as Alice authenticated at time T with IP X. She is issued with a token generated by blockchain. In the case where

Alice attempts to list all cloud servers, the backend of the console invokes the access control contract containing the token of Alice and the listServers action. This is a check that Alice has the role attribute (admin) and the validity of her session token; the request is approved and an entry is made in the log as Alice accessed listServers at time T2. The same action would be denied (and recorded) by the contract had Bob who was a standard developer attempted the same action since he has no role attribute that permits such an action. By doing this, all the authentication, and authorization processes will be authenticated by the aggregate trust of the blockchain network and auditable. An attacker cannot create new permissions or user identities without the collusion of the majority of the blockchain nodes, which would be independently operated, even in case of the internal systems of the cloud provider being compromised.

Scalability Considerations: We do admit that blockchain throughput may be a bottleneck. To deal with this, our architecture would adopt a scalable consortium chain (e.g. Hyperledger Fabric or some variant of Tendermint-based chains) that can support hundreds or thousands of transactions per second, and may group multiple auth events into a single block. We can also decouple the on-chain transactions of not every user action: we can on-chain critical security operations (first login, changing privileges, access to highly sensitive resources), but off-chain accesses with short-lived tokens may be checked with an on-chain attestation that is recent. This mixed methodology decreases load. Such techniques as state channels or layer-2 networks may also offload common interactions, but leave final states attached to the main chain to achieve security.

Integration with Existing Systems: The framework would be configured to work with the cloud provider APIs and support the standard protocols (OAuth 2.0, OIDC, SAML) by serving as the back end to the protocols. To illustrate the example above, an OIDC provider service may be deployed over the blockchain - a client application requests an ID token on behalf of a user, the OIDC service would do the blockchain authentication under the hood and provide a token in case it is allowed. In such a manner, front-end applications may not know anything about the blockchain at all; they are presented with a standard SSO service, but what they do not realize is that it is decentralized in the back-end.

The suggested framework is basically the amalgamation of the strong aspects seen in the literature: the decentralized single sign-on of Yu et al. (2023), the fine-grained smart contract policies of Alatawi (2025), the user-controllable identity of Mostafa et al. (2025), and adaptive security measures such as Zhao et al. (2023) into a model that makes sense. Although the implementation of such a comprehensive system would place a strong focus on the close engineering and cooperation (in particular to form the

consortium of trust), the potential beneficial effects on the security of cloud networks are enormous. It would significantly decrease the number of credential breaches and unauthorized access on a large scale, offer unified cross-cloud trust, and offer more trust and control to users on their digital identities.

Conclusion and Future directions.

A major paradigm shift in cloud network security is the use of blockchain based authentication structures. These frameworks can prevent many risks, including single point of failure, insider attacks, and auditability, by eliminating the need to use centralized identity providers and using instead cryptographically secured and distributed ledgers. As our review of the literature reveals, blockchain technology can be effectively utilized in all the areas of authentication and access control: to establish a form of self-sovereign identity in users, to mediate trust between two or more cloud providers, to record and implement access policies using smart contracts. It is strongly evidenced that these methods could increase the level of security, e.g. it was shown that the probability of unauthorized access and successful defense against the most common attacks is almost impossible in the case of blockchain-based authentication (Alatawi, 2025; Jin and Omote, 2024). Besides, the characteristics such as inbuilt transparency and tamper-evidence help with the compliance and forensic analysis of the incidents.

Nonetheless, there are no issues with this new approach. Scalability and performance are major considerations - authentication systems will be needed to deal with potentially millions of transactions (logins, token validations) per second when the cloud is large. Public blockchains are currently unable to offer that scale at low latency. Some of the suggested solutions are permissioned chain, layer-2 scaling, or on/off-chain hybrid designs. Currently, research is pursuing high-throughput consensus algorithms and sharding schemes that may enable blockchain authentication to be as fast as the current centralized systems (Zhao et al., 2023, using LRaft consensus is one such effort to work on efficiency). Security of the blockchain itself is another issue, although decentralization contributes to resilience, the nodes of the blockchain and smart contracts should be safe. The system could be compromised by bugs in the code of smart contracts or a majority of the consortium validators. This requires close security auditing of contracts and the close management of consortium blockchains (e.g. through the use of a variety of node operators and hardware security modules to secure key protection).

Privacy is very two-sided in these frameworks. On the one hand, users have a greater control over their data on identity, they might present less data to each service (a service can simply check a claim through blockchain without viewing all the data). Conversely, a registry of transactions that cannot be changed

may pose privacy concerns unless it is properly thought out - on-chain personal data cannot be undone. The current research is being directed towards privacy-friendly cryptographic methods such as zero-knowledge proofs, secure multiparty computation, or permissioned ledgers so that it is possible to take advantage of blockchain authentication without breaching privacy laws such as GDPR. Other researchers already enforce zero-knowledge authentication, whereby the blockchain is capable of attesting to an identity proof without knowing the secret or metadata of the user (this may permit, e.g., age or citizenship verification via blockchain in way that is privacy-guaranteed).

The second area that future studies can focus on is combining blockchain-based authentication and new technologies. As an example, what can these frameworks do to facilitate the growing edge computing and the fog case? Others (such as the BDEQ framework in Scientific Reports 2025) use blockchain with AI to arrange trust at the edge - analogous concepts may be generalized to have edge devices implement local blockchain consensus to achieve super-fast authentication in a network such as an autonomous vehicle network or even a smart factory, and anchor summaries to a cloud blockchain. Furthermore, post-quantum cryptography will also need to be added to blockchain identity systems with the emergence of quantum computing, to make them resistant to threats in the future - this could be by replacing the algorithms used to perform digital signatures on the blockchain with quantum-resistant algorithms.

On an industry front, we have early adoption: tech companies and standards organizations are experimenting with decentralized identity (e.g. ION network on Bitcoin in Microsofts DID implementation, the activities of the Decentralized Identity Foundation). In the near future, cloud providers may be selling so-called Blockchain Identity as a security service, similar to their management blockchain services. The effectiveness of these structures will be determined by the realization of interoperability (where a user blockchain identity can be interpreted by services and providers in a seamless manner) and showing the overall benefits of these systems over traditional ones in actual implementation.

To sum up, authentication frameworks based on blockchain can contribute to the substantial improvement of the security of the cloud network by decentralizing trust, and integrating security into the structure of authentication transactions. Though the issue of scalability, privacy, and complexity can still be encountered, the high rate of research (with numerous solutions reported within the past few years) is bridging these gaps. We believe that components of these models - especially decentralized identity and blockchain-based audit logs - will slowly be integrated into more traditional cloud security models, as the

industry moves to a more robust, user-oriented, and trust minimized identity and access management model..

References:

- Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., & Lutfi, A. (2023). *A new blockchain-based authentication framework for secure IoT networks*. Electronics, 12(17), 3618. https://doi.org/10.3390/electronics12173618

- Alatawi, M. N. (2025). *Blockchain-Driven Smart Contracts for Advanced Authorization and Authentication in Cloud Security*. Electronics, 14(15), 3104. https://doi.org/10.3390/electronics14153104

- Deep, G., Mohana, R., Nayyar, A., Sanjeevikumar, P., & Hossain, E. (2019). *Authentication protocol for cloud databases using blockchain mechanism*. Sensors, 19(20), 4444. https://doi.org/10.3390/s19204444

- Jamal, F., Gondal, I., & Jo, J. (2019). *Dynamic trust management framework using blockchain for zero trust networks*. **(Details of publication)**.

- Jin, X., & Omote, K. (2024). *An efficient blockchain-based authentication scheme with transferability*. PLoS ONE, 19(9), e0310094. https://doi.org/10.1371/journal.pone.0310094

- Khanna, A., et al. (2022). *Blockchain–Cloud integration: A survey*. **(Journal)**, 12(??), Article 1295. https://doi.org/10.3390/???? **(Placeholder for actual journal details)**

- Mostafa, A. M., Mohamed, E. R., Hanafy, A., Alserhani, F., et al. (2025). *Decentralized Identity Management in Cloud Computing: A Blockchain-Based Solution With Automatic Provisioning Techniques*. International Journal of Intelligent Systems, 2025(1), e2969737. https://doi.org/10.1155/int/2969737

- Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). *A survey on essential components of a self-sovereign identity*. **Technology Innovation Management Review / Computer Science Review**, 30, 80-86. **(Replace with actual journal reference)**

- Novo, O. (2018). *Blockchain meets IoT: An architecture for scalable access management in IoT*. IEEE Internet of Things Journal, 5(2), 1184-1195. https://doi.org/10.1109/JIOT.2018.xxxxx

- Pham, H.-A., Nguyen, C. T., & Lam, T. C. (2025). *Blockchain adoption for authentication: A survey*. Blockchain: Research and Applications, **(in press)**,100383. https://doi.org/10.1016/j.bcra.2025.100383

- Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). *A systematic review on blockchain-based access control systems in cloud environment*. Journal of Cloud Computing, 13(1), Article 146. https://doi.org/10.1186/s13677-024-00697-7

- Saleem, T., Janjua, M. U., Hassan, M., Ahmad, T., Tariq, F., Hafeez, K., et al. (2022). *ProofChain: An X.509-compatible blockchain-based PKI framework with decentralized trust*. Computer Networks, 213, 109069. https://doi.org/10.1016/j.comnet.2022.109069

- Sharma, P. K., & Park, J. H. (2018). *Blockchain-based hybrid network architecture for the smart city*. Future Generation Computer Systems, 86, 650-655. https://doi.org/10.1016/j.future.2018.04.040

- Yu, L., He, M., Liang, H., Xiong, L., & Liu, Y. (2023). *A blockchain-based authentication and authorization scheme for distributed mobile cloud computing services*. Sensors, 23(3), 1264. https://doi.org/10.3390/s23031264

- Zhao, H., Zhang, Y., Fang, J., Chen, X., & Qian, Y. (2023). *Blockchain-based authentication scheme with an adaptive multi-factor authentication strategy*. Mobile Information Systems, 2023, Article ID 6691243. https://doi.org/10.1155/2023/6691243