Kurdistan Journal of Applied Research (KJAR)
Print-ISSN: 2411-7684 | Electronic-ISSN: 2411-7706

Review Article

Check for updates

A Comprehensive Review and Analysis of Blockchain-Based Security Solutions for Cloud Computing Ecosystems

Noor Ghazi M. Jameel [a], **Zryan Najat Rashid** [a *], **Abdulkadir Şengür** [b]

[a] Department of Computer Networks, Technical College of Informatics, Sulaimani Polytechnic University, Sulaymaniyah, Iraq.
[b] Firat University, Technology Faculty, Electrical and Electronics Engineering Department, Elazig, Turkey.

Submitted: 23 February 2025
Revised: 28 March 2025
Accepted: 24 May 2025

* **Corresponding Author**: zryan.rashid@spu.edu.iq

Keywords: Blockchain, Cloud computing, Data security, Identity management, Authentication, Access control.

How to cite this paper:
N. G. M. Jameel, Z. N. Rashid, and A. Şengür, "A Comprehensive Review and Analysis of Blockchain -Based Security Solutions for Cloud Computing Ecosystems", KJAR, vol. 10, no. 1, pp. 126–145, May 2025. doi: 10.24017/science.2025.1.9

Abstract: Cloud computing is a rapidly evolving technology that defines a modern digital computing framework and business approach for utilizing software and hardware resources. While it provides numerous advantages, it also brings with it considerable security risks and challenges. This paper discusses cloud computing and blockchain technology with a focus on the security implications of integrating these two technologies for solving three security issues in the cloud environment. Three major security domains—data security, identity authentication and management, and access control—have been analyzed through an in-depth review of recent studies to evaluate the strengths of integrating both technologies, identify existing limitations, and propose suggestions for future research directions. Relevant literature was retrieved from five major scientific databases: Google Scholar, ScienceDirect, IEEE Xplore, Scopus, and Web of Science. The selection of studies was guided by predefined research questions and specific inclusion and exclusion criteria. The findings reveal that the combination of blockchain and cloud computing establishes a new era of enhanced security. This fusion of blockchain and cloud computing represents the most promising path forward, offering robust security with decentralization and delivering significant advancements in authentication, authorization, data integrity, and privacy protection. This approach will open up vast opportunities in various sectors like healthcare, business, supply chain, and industry due to its guaranteed data security, improved efficiency, and reduced costs. Future research areas need further investigation, such as designing innovative consensus mechanisms to boost scalability and leveraging artificial intelligence and machine learning to improve security and privacy by incorporating blockchain technology into cloud environments.

1. Introduction

Recently, cloud computing has become a breakthrough technology in the contemporary area of technological innovation for individual handling and data processing at the organizational level. As with any computing resources in a need-driven process, cloud computing provides easier ways to have access to such resources: storage facilities, processing powers, or networking. Therefore, increased flexibility, scalability, and cost-efficient results has been observed. This kind of technological paradigm has

enabled different companies to scale their business accordingly and minimize their infrastructure expenses toward their core businesses rather than channelizing business operations through the maintaining processes of hardware administration [1].

A comprehensive search was conducted across the Google Scholar, Science Direct, IEEE Xplore, Scopus, and Web of Science databases for articles published between 2015 and 2024. The search terms included 'blockchain', 'cloud computing', 'cloud security', and 'integration'. The inclusion criteria focused on peer-reviewed studies that examined the use of blockchain in cloud environments. Non-English publications, non-published articles and studies unrelated to security were excluded.

While cloud computing has become integral to the modern Information Technology (IT) infrastructure, one of the biggest concerns is related to security. Cloud computing security can be defined as all policies, technologies, and controls that are specifically designed to protect data, applications, and infrastructure against a probable cyber threat. The challenge lies in securing a distributed environment where data is usually stored remotely, often spread over multiple regions and jurisdictions, along with increasing vulnerability to potential data breaches, unauthorized access, and service disruptions [2].

While blockchain technology has been synonymous with cryptocurrencies, it has grown out of its original use case to extend an additional layer of security to many other industries. Blockchain technology allows secure, intermediary-free data transactions by creating a decentralized, immutable ledger. The transparency and cryptographic security mechanisms involved make blockchain very attractive for building trust in digital transactions, especially in environments where data integrity is paramount [3].

The convergence of cloud computing and blockchain opens up whole new dimensions regarding innovation and enhancing the security level of the cloud environment. Ensuring more robust data integrity, user authentication, access control and transaction verification can be done by leveraging the decentralized architecture from blockchain, improving the cloud framework's security. This review study explores the potential crosslink between the mentioned key technologies, presenting various discussions regarding numerous solutions and open points related to the adoption of cloud environments with blockchain-based methodologies for solving the issues present in three main security domains.

Although numerous studies have discussed the individual potential of blockchain and cloud computing, there is a lack of comprehensive studies evaluating how blockchain technologies can systematically address specific security solutions and gaps in cloud environments. This study aims to (1) explore the existing research on blockchain-based cloud security solutions, (2) identify key limitations and gaps, and (3) propose a future research agenda.

The rest of this paper is structured as follows. Section 2 provides the background information covering the concept of cloud computing, its benefits, and associated security challenges. It also introduces blockchain technology, including its components and security features. Section 3 outlines the methodology adopted in this study. Section 4 addresses the research questions through a comprehensive review and analysis of security solutions that integrate blockchain with cloud computing, focusing on three key areas: data storage and transfer, identity authentication, and access control. Finally, Section 5 presents the study's findings.

2. Background

2.1 Cloud Computing

Cloud computing enables easy, on-demand network connectivity by utilizing a shared pool of programmable computer resources that can be instantly installed and released with minimal administrative effort. In its most basic form, cloud computing is the use of an online platform to offer storage and hosting services together with other technological elements [4]. When it comes to the internet economy, cloud computing is among the most rapidly expanding sectors. It has evolved into a paradigm for hosting and delivering services online, allowing users to access data, apps, and services from any location via an internet-connected device [5]. It is a form of computing where IT-enabled capabilities are offered "as a service" through Internet technology, according to researchers. It has numerous everyday applications, like as Gmail, Dropbox, and Microsoft Office 365 [6]. It is ranked first among the 10

most significant innovations of all time, indicating that it is a critical and potentially transformative technology [5].

Rapid innovation, resource adaptability, and cost savings through economies of scale are made possible by cloud computing. This utility-driven, pay-per-use technology eliminates the necessity for local servers or personal devices to manage applications [7]. To satisfy user demands, the system's architecture depends on the functioning of networks of distant servers and storage devices, such as data centers and server farms [8]. Businesses can save time and money by eliminating the necessity for physical infrastructure. Cloud service providers, including Microsoft, Amazon, and Google, maintain and store client data in their server centers, and the distributed computing is entirely web-based [9].

Cloud computing presents significant security and privacy issues and concerns despite its many benefits, which include cost reductions, shared resources, and data storage. The digital computing paradigm and commercial models for hardware and software resources are exemplified by cloud computing [10, 11]. When thinking about cloud security, we should concentrate on typical security problems and difficulties like security concerns with stored and transferred data, where data on the cloud is kept on various servers in various places. Network storage that is dispersed presents a security challenge. To authenticate users at any moment, the cloud provider must make the storage data available and capable of managing this kind of security issue. Malicious actors can take advantage of the vulnerabilities created by the movement and storage of enormous volumes of data in cloud systems [11, 12]. Problems with application security are where the cloud allows multiple users to access applications. This application's security is a major problem since cloud applications are used by hackers to steal data and launch malicious assaults against it. A suitable, secure framework should be available to access cloud apps from different platforms. Problems with user identity security relate to the cloud offering customers on-demand services including data storage and access to various resources, apps, and networks. The difficulty here is in controlling authorized customers. Prior to offering the service, it is essential to verify the user's identification. Malicious users run the risk of posing as trustworthy ones in order to get access to and contaminate the cloud. Many customers who share the impacted cloud could be affected by this [12, 13]. Because the users of cloud systems are given different privileges to access sensitive data, access management is another crucial issue. Users no longer have complete control over their security settings and sensitive data. Cloud providers may also gain access to customer data, in addition to the attackers. Protecting user privacy is a crucial duty for cloud providers to guarantee the security of user data [14]. Access management policy [12] authorization, and authentication can be used to ensure that only the appropriate user has access to specific resources.

It is essential to address cloud computing security. Inadequate security measures for data storage, operations, and transmission substantially heighten the risks to data integrity and privacy. In a cloud-based internet paradigm, it is imperative to prioritize data security and confidentiality as data loss, leakage, or tampering can seriously damage a business's brand and credibility [13].

For instance, the 2019 Capital One breach exposed over 100 million customer records due to a misconfigured web application firewall on Amazon Web Services (AWS). Similarly, the 2016 Dropbox incident, where credentials from third-party apps led to the leak of 68 million passwords, underscores the importance of robust cloud security mechanisms [15, 16].

2.2 Blockchain Technology

Blockchain is a decentralized digital ledger composed of interconnected blocks that store data in a secure, immutable format [17].

A significant differentiator and competitive edge among cloud services is being created by cloud protection. The use of blockchain technology is currently among the well-liked inventions that can solve the security concerns to do with cloud computing. Blockchain is a transparent, decentralized digital ledger system that provides anonymity, security, and data integrity without the need for a third party. Since the introduction of Bitcoin, blockchain technology has gained popularity. The finance industry is not the only one using this technology [18]. Numerous stakeholders, including those in the government, real estate, infrastructure, finance, and healthcare sectors, place a high importance on blockchain technology. The foundation of blockchain-based systems is a distributed, integrated, and fault-tolerant

ledger structure that is available to all network participants while not being controlled by any of them. The service provided by the blockchain network is therefore independent of a centralized, trustworthy third party [19]. By removing middlemen, facilitating peer-to-peer transactions with greater confidence, and offering improved security, traceability, and efficiency, it has the potential to completely transform industries [20].

Blockchain networks consist of blocks of data, smart contracts, consensus, and a distributed ledger [21]. They ensure transactional data integrity and availability through cryptography, with each block containing a timestamp, encrypted hash, and block hash. Blockchain can be defined as a distributed ledger that addresses privacy concerns by safeguarding data and validating all network members. It stores data over a peer-to-peer network, providing enhanced security and transparency [22]. The consensus mechanism is an algorithm which makes sure that only legitimate transactions are recorded in the ledger, such as proof-of-work and proof-of-stake [20]. Contracts that are self-executing and coded on a blockchain are referred to as smart contracts. Under certain circumstances, the terms and conditions of a transaction are automatically enforced when certain prerequisites are satisfied. The use of smart contracts makes it possible to conduct transactions that are both programmable and automatic, eliminating the need for intermediaries. This has the potential for enhanced efficiency, transparency, and confidence in decentralized applications [23]. The use of this strategy guarantees that any unauthorized changes will be discovered and corrected without delay [24].

Blockchain is utilized to safeguard models that have been developed in a broad variety of fields [25]. For a cloud-based architecture to be in compliance with the law and the standards for data protection, data security is absolutely necessary [26]. One approach that might be taken to improve the safety of data stored in cloud computing systems is the implementation of blockchain technology. This technology provides a decentralized, immutable record system that guarantees integrity, transparency, and resistance to tampering. The primary application of this technology was originally to power cryptocurrencies such as Bitcoin. Businesses have the ability to strengthen their defenses against a variety of security problems that are frequent in cloud computing by utilizing the distinctive qualities of blockchain technology [27]. Blockchain can be combined with cloud computing to generate an immutable cloud-based data processing and storage system [28]. The smart contracts that are used by cloud data nodes make it possible to collect and store data in a reliable and correct manner. There is potential in blockchain technology but, as of yet, it does not have the capacity to store information to its fullest potential. There is a possibility that it is not viable to store massive data sets on it due to its lack of scalability [29].

Research in a number of theoretical and practical domains is still running strong because of the necessity for blockchain development and the importance of its application. Although the blockchain is still in its infancy, it is already being viewed as a progressive solution to contemporary technological problems including decentralization, identity, trust, data ownership, and information-based decision-making. When looking for the best way to store and access cloud data, the blockchain innovation provides substantial insights [30].

Blockchain technology has gained attention in recent times owing to its ability to revolutionize traditional trade through its distributed ledger attribute. The prompt advancement of blockchain demands new systematic studies to investigate and analyze the existing knowledge in this domain [31].

3. Materials and Methods

This section outlines the stages of the study's methodology. The primary steps include identifying relevant studies, screening the gathered research, extracting data from the chosen studies, and ultimately reporting and presenting the results.

3.1 Research Questions

This study seeks to analyze recent research, evaluate the methods used, and summarize the findings regarding the application of blockchain technology to improve cloud computing security. To accomplish this objective, we have formulated the following research questions, guided by our review of the relevant literature and aligned with the study's intended contributions:

- RQ1: What is the distribution of the specified studies based on the year of publication?
- RQ2: What are the security domains and existing solutions that have used blockchain for enhancing cloud computing security?
- RQ3: What are the limitations of the existing solutions?
- RQ4: What are the prospective directions for future research in leveraging blockchain technology to enhance the security of cloud computing systems?

3.2 Search Strategy

This study focuses on improving the security of cloud computing through the application of blockchain technology. The scope of the reviewed literature spans from January 2015 to December 2024. Relevant scholarly publications were systematically retrieved using automated searches across multiple academic databases—namely Google Scholar, ScienceDirect, IEEE Xplore, Scopus, and Web of Science—employing keywords derived from the formulated research questions.

3.3 Inclusion and Exclusion Criterion

This stage outlines the inclusion and exclusion criteria applied in this study. First, journal articles, conference proceedings, master's and doctoral theses or dissertations, and book chapters were included, while excluding other sources such as books, editorials, reports, and reference materials. Second, duplicate entries identified across all databases were removed. Finally, each publication was assessed to determine its relevance, resulting in the final selection of studies that specifically address the use of blockchain to enhance cloud computing security. Figure 1 illustrates the detailed stages of the methodology.

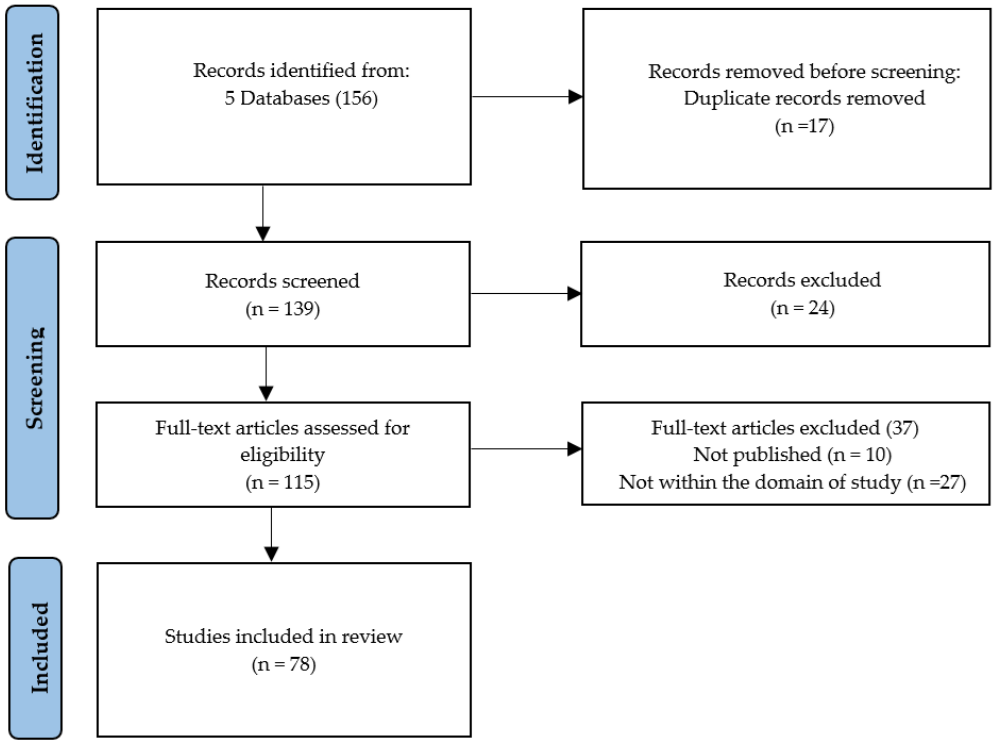

Figure 1: The stages of the study's methodology.

3.4 Data Extraction

This phase describes the data extraction process, which involved a thorough review of all selected studies. Relevant information was systematically extracted using Microsoft Excel and Mendeley Reference Manager. An Excel spreadsheet was used to organize and record the extracted data from each

study. The collected information included bibliographic details—such as paper title, authors, publication source, and year of publication—as well as the study's objective, applied techniques or mechanisms, the addressed security domain, the main strengths, and any identified limitations. The selection of these data elements was guided by the research objectives and corresponding research questions.

3.5 Data Reporting

The data derived from the evaluation of the reviewed studies was thoroughly analyzed and presented in tabular form using Microsoft Excel with the aim of identifying each study's objectives, employed techniques, and key strengths.

4. Discussion

This section presents the detailed results of the review, with the research questions being addressed based on the findings from the analyzed studies.

4.1 RQ1: What is the Distribution of the Specified Studies Based on the Year of Publication?

Figure 2 illustrates the distribution of selected studies according to their year of publication. The line graph in Figure 2 indicates a significant increase in the number of studies on the topic, particularly in 2023, reflecting a growing interest in applying blockchain technologies to enhance cloud security. However, in 2024, the number of publications decreased from 16 in 2023 to 8 in 2024. This decline can be attributed to the unavailability of certain publications for download as they are not open access.

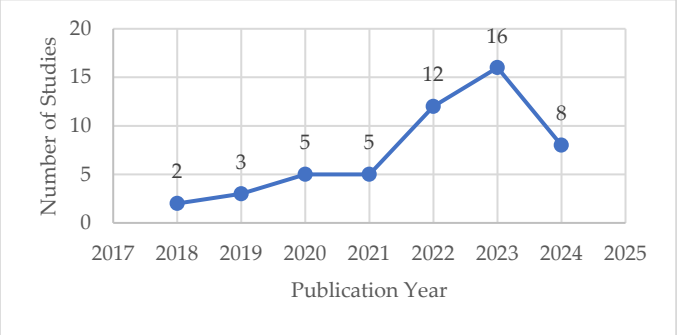

Figure 2: Distribution of the selected studies by year of publication.

4.2 RQ2: What are the Security Domains and Existing Solutions that have Used Blockchain for Enhancing Cloud Computing Security?

Strategies for integrating blockchain into cloud security focus on utilizing blockchain technology to strengthen the protection of cloud computing environments. These approaches aim to tackle critical security challenges in cloud computing including data privacy, integrity, identity verification, access management, and regulatory compliance [23].

Integrating blockchain technology into cloud computing brings significant benefits. The key advantages are decentralization, enhanced data security and user privacy, improved identity management and access control mechanisms [32]. Additionally, it offers greater transparency and traceability, facilitating compliance with regulatory requirements, and enables secure transactions and agreements by improving the cloud computing services' efficacy and efficiency [33]. By leveraging the benefits of both cloud computing and blockchain technology, organizations can enhance the security and trustworthiness of their cloud infrastructure [20].

In July 2024, the Cloud Security Alliance released the "Security Guidance for Critical Areas of Focus in Cloud Computing v5.0" [34], outlining 12 key areas of focus for cloud computing security. This study conducted an extensive literature review and then classified and examined various mechanisms and solutions that utilize blockchain technology to strengthen three fundamental aspects of cloud computing security: data protection, identity verification, and access control management.

A. Blockchain for Enhancing Cloud Data Security in Rest and Transit

The widespread use of the Internet has made cloud services the dominant platform for storing and sharing data. While this advancement offers convenience, it has also heightened concerns over privacy and data security. The existing security countermeasures engaged by cloud service providers remain susceptible to cyberattacks and data breaches. Furthermore, traditional centralized security solutions are increasingly inadequate for defending against these threats. To safeguard sensitive information in cloud systems, innovative and robust security measures are crucial. Blockchain technology, with its decentralized and inherently secure design, offers a promising solution to these challenges by introducing a novel approach to ensuring data privacy and integrity in cloud environments [27].

Various recent studies have been reviewed to examine the integration of blockchain technology with cloud computing for securing data in cloud storage and during transmission. Their goals, techniques, and key strengths are summarized in table 1.

In a study by Zhang *et al*. [35], the authors provided a conceptual plan for using blockchain and cloud storage technology to communicate ongoing personal health data. To keep control over the data quality, the article also presented a machine learning-based data quality inspection module. This method offers a practical means of collecting superior personal health information for both commercial and research determinations.

In the study by Mohammed [36], the author proposed utilizing blockchain for electronic health records (HER) in the healthcare industry. Strong security was offered by the suggested work for data sharing and storage with low processing demands.

In a study by Awadallah *et al*. [28], the authors proposed a scheme for preserving data confidentiality that integrated blockchain, cloud computing, and homomorphic encryption. The suggested scheme makes use of the Byzantine Fault Tolerance consensus method to lessen the centralized control that cloud service providers (CSPs) have over data. By creating a dispersed network of processing CSPs based on customer needs, this method guarantees data integrity and makes it possible to identify any instances of data manipulation.

The study by Meenakshi [37] presented a secure and effective method for cloud storage that makes use of software defined networks (SDN) and blockchain technologies. Regarding throughput, computation time, and response time, the SDN module performed well. The Fabricator, Merchant, and Customer (FMC) relationship was established by the blockchain module, which produced better outcomes than conventional models.

Motupalli [38] introduced a hybrid algorithm that integrates a double encryption substitution technique with the Secure Hash Algorithm (SHA)-512. Their algorithm demonstrated higher efficiency in ensuring data security and confidentiality compared to existing methods.

In the study by Amanat *et al*. [39], the authors proposed a secure and decentralized peer-to-peer framework to facilitate secure HER sharing among various electronic healthcare systems. The framework leverages a distributed Hyperledger employing a PoS consensus mechanism alongside the SHA-256 to protect the patients' confidential information. For record verification and secure transactions, the Elliptic Curve Digital Signature Algorithm is utilized. The proposed solution showed better performance than other existing frameworks.

In a study by Rani *et al.* [40], the authors proposed an Internet of Things (IoT) design, integrating cloud and blockchain technologies to deliver decentralized, transparent and safe storage solutions. Beyond the standard layers found in traditional IoT architectures—perception, network, processing, and application layers—the proposed design introduces the service layer, the security layer, and the parallel management and control layer as additional layers. The purpose of these additional layers is to improve the overall security and administration of IoT ecosystem. The suggested architecture provides useful applications and can be used to create smart infrastructures in both the public and private sectors.

The study by Gousteris *et al*. [41] proposed a framework that combined the Rivest-Shamir-Adleman (RSA) encryption and authentication system with the Ethereum blockchain and its smart contracts. Within this framework, RSA encryption protects sensitive data secrecy and authenticates the

source, while the Ethereum blockchain serves as a data structure to guarantee data integrity and availability. This suggested structure guarantees strong authentication verification, makes file sharing easier, and permits safe cloud data storage.

Gou and Deng [42] proposed a blockchain-based encryption approach to protect cloud accounting data. The suggested solution stores and backs up user accounting data, together with its hash value, using blockchain technology. It uses an evidence chain and Elliptic Curve Cryptography (ECC) technology to improve cloud data security and integrity, giving consumers a safer online accounting experience.

In the study by Saah *et al*. [43], the authors designed a blockchain system architecture that integrates the Hyperledger Fabric blockchain with AWS cloud platform to protect the confidentiality and privacy of personal information for construction workers. The outcomes validated the suggested model's viability and operational efficacy.

Abubakar *et al.*[44] used cloud storage to store the actual health reports, and MetaMask, a digital wallet, to buy and connect to the Ethereum blockchain to secure health report linkages. Ethereum blockchain transaction prices were predicted using Recurrent Neural Network (RNN) and Long-Short Term Memory (LSTM) models, providing users with insightful information about possible system effects and market trends. Smarter, more secure applications in the healthcare sector are made possible by the synergistic interaction created by the integration of blockchain and artificial intelligence (AI) technologies.

In the study by Shrivastava and Patel [45], the authors proposed an enhanced security of Hadoop Distributed File System (HDFS). The Hyperledger Fabric blockchain platform was used to ensure trustworthy data security and traceability in HDFS. The results displayed increased performance and reliable data protection.

In a study by Rashmi *et al*. [46], the authors employed the Advanced Encryption Standard (AES) 256-bit encryption algorithm to safeguard user data and maintain confidentiality. The encrypted data is distributed and stored across network peers using the InterPlanetary File System (IPFS). This system mitigates the privacy and security risks linked to centralized cloud storage while allowing peers to monetize their unused storage space by earning cryptocurrency, enhancing storage resource efficiency.

Gund *et al*. [47], the study introduced blockchain-base secure data uploading and downloading processes for more secure deduplication in a cloud storage system that uses efficient cryptographic methods to secure the cloud storage. The replicated data is verified with blockchain procedures with smart contracts. An Attribute-based Role Key Generation Method (ARKG) was applied to create key roles prior to data uploading for data access by authorized users. Message Locked Encryption (MLE) is used to encrypt the data for the data owner to upload it to their CSP.

Guo *et al*. [48], the authors introduced a blockchain-based Hybridized Data-Driven Cognitive Computing (HD2C) model, integrating the blockchain consensus mechanism with Federated Learning (FL). This approach incorporates smart contracts alongside the Proof of Authority (PoA) algorithm to improve security and operational efficiency. Extensive analysis of industrial IoT datasets has demonstrated the superiority of the HD2C model. In comparison to other consensus algorithms, the foundational cost of the PoA blockchain was notably higher. However, evaluations of memory utilization and accuracy highlighted the overall benefits and advantages of the system.

Rajawat *et al*. [49] proposed a system that leverages the cloud for hosting business applications and services while utilizing blockchain to securely record and validate transactions. Smart contracts facilitate payment processing and transaction management, ensuring transparency and trust.

Huang and Yi [50], in order to get around the drawbacks of conventional systems that depend on reliable third-party servers, a blockchain-based key security management system for cloud storage was presented. Their method splits the convergent key into several pieces using a secret sharing technique, which are thereafter controlled by the blockchain network. This method improves security for key management procedures, offers fault tolerance, and guarantees dependable key management.

Kathole *et al*. [51] designed a secure integrated storage system for the cloud that federates a composite empirical Attribute-based Encryption (ABE) strategy with approval blockchain. To increase data secrecy and honesty, the arrangement gathers medical information and scrambles it using ABE, utilizing an ideal key established by the Hybrid Mexican Axolotl with Energy Valley Optimizer (HMO-

EVO). The scrambled data is then firmly stocked within the permissioned blockchain. For methodical healthcare nursing, integrated learning is occupied alongside a Multi-Scale Bi-Long Short-Term Memory and Gated Recurrent Unit (MBiLSTM-GRU) model, which prognoses complaints.

Table 1: Blockchain-cloud integration for enhanced data security.

Source	Year	Research Goal	Used Techniques and Technologies	Strengths
[35]	2018	To allocate health-linked facts in a steady and translucent approach.	Blockchain, Cloud Computing, and Machine Learning technologies.	• Safe exchange of personal health information.
[36]	2020	To display a Blockchain-Based Healthcare System (HS-BC) with burly safety and less reckoning proceeding.	Blockchain, Cloud Computing.	• Strong security for data storage and sharing. • Improved performance. • Lower latency compared to conventional systems.
[28]	2021	To maintain data confidentiality and integrity in cloud computing.	Homomorphic encryption, Blockchain, and Cloud computing.	• Less expensive than using Ethereum. • Efficient online performance.
[37]	2022	To provide security for the online transactions among FMC.	SDN, Blockchain and Cloud computing.	• Improved throughput. • Reduced computational, and response time.
[38]	2022	To locate a productive protection algorithm to defend the data secretly and the aloneness of each separate user in the cloud habitat.	Substitutional algorithm, SHA-512, Blockchain, and Cloud computing.	• High throughput. • Efficient in ensuring data confidentiality and security.
[39]	2022	To provide secure and efficient sharing and storage of EHR on the cloud.	SHA-256, ECDSA, Blockchain, and Cloud computing.	• Secure healthcare data storage and exchange. • Improved efficiency in throughput, computation and communication costs.
[40]	2022	To provide advanced and efficient storage and security solutions to the IoT ecosystem.	IoT, Blockchain, and Cloud computing.	• Advanced security. • Prevents single points of failure. • Cost-effective communication.
[41]	2023	To provide secure data storage and sharing over cloud storage infrastructures.	RSA, Blockchain, and Cloud computing.	• Secure data storage and file sharing.
[42]	2023	To address the data security and integrity issues faced by cloud accounting.	ECC, Blockchain, and Cloud computing.	• Low computational overhead. • Improved user authority over cloud accounting data. • Secure data transfer. • Strengthens the user and cloud accounting service providers' trust.
[43]	2023	To enhance the privacy and safety of construction workers' personal information.	Blockchain, and Cloud computing.	• Provides decision-making for high-risk activities. • Enhanced data security and privacy. • Promotion of industry innovation and trust.
[44]	2023	To ensure confidentiality and integrity while enabling the efficient exchange of medical information.	RNN, LSTM, Blockchain, and Cloud computing	• Safe and effective sharing and preservation of medical records. • Improved decision-making processes. • Enhanced patient outcomes. • Optimized operations. • Lower costs.
[45]	2023	To improve the security of HDFS by blockchain technology.	HDFS, Blockchain, Cloud computing	• Increased performance. • Reliable data protection.
[46]	2023	To leverage idle storage resources and reduce the costs associated with dedicated infrastructure	AES, Blockchain, and Cloud computing.	• Enhanced data security. • Maximized storage resource utilization.

Table 1: Continued

[47]	2023	To secure deduplication in a cloud storage system with a high deduplication rate and throughput.	ARKG, MLE, Blockchain, and Cloud computing.	• High throughput. • Reduced deduplication elimination ratio.
[48]	2023	To enhance the IoT infrastructure's security and performance in a complex environment.	FL, Blockchain, and Cloud Computing.	• Increased data security. • Resistance against poisoning assaults in the IoT sector. • Improved computational processing efficiency.
[49]	2024	To increase the security of electronic banking payments.	Blockchain, and Cloud computing.	• Improved security of electronic banking. • High transaction processing speed. • Cost saving compared to traditional infrastructure.
[50]	2024	To achieve a secure and reliable key management scheme.	Blockchain, and Cloud computing.	• High safety. • Resistant against brute-force attacks and conspiracy attacks. • Low time calculation overhead.
[51]	2024	To secure patient information and accurately predict diseases in hospitals	ABE, Blockchain, Cloud computing, and FL with MBiLSTM-GRU.	• Secure medical data management. • Good efficacy and predictive accuracy.

Based on the intensive review of the literature, the integration of blockchain with cloud computing provides improved security for data storage and transmission which has led to the widespread use of this combination across multiple domains, including the financial industry, construction, healthcare, and IoT ecosystems. The distributed characteristics of blockchain have also provided a solution to the security issues in the cloud to protect single points of failure. In addition, advanced and reliable cloud environment with integrated blockchain technology have introduced improved performance in throughput, computation, and communication costs.

B. Blockchain for Improved Cloud Identity Authentication and Management

Identity authentication and management is the process of verifying the authenticity of the party. The idea is that the authenticating party validates the characteristic information of the authenticated party to confirm its validity and effectiveness [52]. Identity authentication and management play a vital role in cloud computing security by ensuring that only authorized individuals can access data and resources. Traditional methods are centralized and rely on a single authority to handle user identities, making them prone to security breaches. However, existing identity management systems are still not secure or reliable enough to fully protect against potential threats [53].

Authentication in cloud services can be done using different mechanisms. Some mechanisms leverage biometric authentication, such as fingerprint scanning, iris detection, and face recognition, while others rely on digital security methods like passwords, single sign-on (SSO), and multifactor authentication [54]. Identity authentication and management can be achieved safely and decentralized with the help of blockchain.

Blockchain technology offers many benefits for identity management and authentication. First, identity management systems built on blockchain offer improved privacy and security. Since blockchain is decentralized, data is safe against identity theft, hacking and single points of failure. Blockchain-based identity management solutions also use cryptography to protect user data confidentiality and integrity. Second, blockchain-based identity management systems provide a user-centric approach. Users have control over who can access their data and can remain in charge. This approach empowers individuals while enhancing their privacy and autonomy. Thirdly, blockchain-based identity management systems provide interoperability and portability. Users can use their digital identities across several systems and platforms without having to remember multiple usernames and passwords [55].

Currently, there is a significant amount of researches on blockchain-based identity authentication applied for cloud environment. This section, along with table 2, classifies the reviewed studies based on their objectives, applied methodologies, and main strengths.

Bendiab *et al.* [56] presented a blockchain-based method for managing cloud identities that improves security and dependability by combining a decentralized trust model and an authentication mechanism. The suggested paradigm offered a practical way to establish safe Infrastructure as a Service (IaaS) cloud federations.

In the study by Deep *et al*. [57], a new authentication method based on blockchain to control both insiders and outsiders in the cloud was proposed. The user's credentials are first validated, then the blockchain node parameters are examined. To assess the system's resistance to various attacks, the Scyther formal system tool was used. The results showed that the suggested solution was very successful in handling both external and internal threats, enhancing cloud security by identifying and thwarting a number of possible attacks through its authentication procedure.

In a study by Wang *et al*. [58], the authors suggested the Ethereum-based Identity Management (EIDM) protocol, a cloud user identity management system built on the Ethereum blockchain. The Consolidated Identity Management (CIDM) protocol is improved by this protocol. The improved version introduces JSON Web Tokens in OAuth 2.0, which allows the integration of smart contracts into the EIDM protocol. Additionally, to guarantee that the protocol can provide trustworthy and legitimate identity identification for cloud customers and service providers, a credit management mechanism was implemented.

The study by Kebande *et al*. [59] proposed a Blockchain-based Multi-Factor Authentication paradigm for cloud-enabled Internet of Vehicles (IoV) and vehicular clouds with an embedded digital signature (MFBC_eDS). This architecture supports a networked edge-to-cloud ecosystem by integrating SSO functionality with the Security Assertion Markup Language. The model's assessment revealed that it offers a strong security solution, greatly boosting the safety of IoT-to-cloud connected vehicles.

Vivekanandan *et al*. [60] proposed a user authentication methodology based on blockchain technology that protects privacy in a distributed mobile cloud setting. With this system, mobile users can access several CSPs after registering once via blockchain. Blockchain technology is used to conduct authentication between the mobile user and the CSP. For added security, the protocol uses the SHA-1 and ECC algorithms. It successfully defends against every known attack, and performance tests show that it outperforms the current protocols in terms of efficiency and security.

In a study by Prasad and Rekha [61], the study proposed a blockchain-based Identity Authentication System protocol to enhance cloud computing security and privacy. The protocol guarantees a decentralized, tamper-resistant method of confirming the integrity of virtual machines in cloud settings by leveraging blockchain technology. The suggested method outperformed other algorithms in a number of performance indicators, such as energy usage, end-to-end latency, message delivery ratio, and data access rate.

The study by Du *et al*. [62] suggested Hyperledger Fabric Identity Authentication, a secure and effective authentication method that combines blockchain and zero-knowledge proof technologies. In cloud computing scenarios, this approach enables safe and effective user authentication to service providers, providing improved security while optimizing performance.

According to Fang *et al*. [63], a distributed industrial data trading architectural model was introduced. The model uses cloud and blockchain technology and is suitable for situations with many data owners. By using smart contracts and a publicly verifiable data integrity mechanism to ensure data integrity across many owners, the model creates a fair trading system for industrial datasets without relying on a reliable third party. Additionally, the concept incorporates threshold tracking and verifiable credentials with selective disclosure, offering privacy-enhanced authentication and the capacity to track malicious individuals.

Table 2: Blockchain-cloud integration for improved identity authentication and management.

Source	Year	Research Goal	Used Techniques and Technologies	Strengths
[56]	2018	To introduce a trust and identity management model for the cloud.	Blockchain, and Cloud computing.	• Effective identity management solution. • Improved security and privacy.
[57]	2019	To provide a secure authentication mechanism for cloud databases.	Blockchain, and Cloud computing.	• Efficient and successful at mitigating various outsider and insider threats. • Robust in real-time working environments.
[58]	2019	To address the issue of the excessive third-party-centricity of existing identity management systems.	Blockchain, and Cloud computing.	• Solved the problem of over-reliance on third parties. • Security guarantee relative to the CIDM protocol. • Practical and flexible.
[59]	2021	To provide adequate and effective authentication technique for vehicular clouds and cloud-enabled IoV.	Blockchain-based Multi-Factor authentication model, and Cloud computing.	• Suitable in countering major adversarial attacks in an IoV-centered environment. • Ensuring the key principles of the Confidentiality, Integrity, and Availability (CIA) triad.
[60]	2021	To move the information management task from the centralized server registration to public blockchain.	SHA-1, ECC and Blockchain, and Cloud computing.	• Secure from all known attacks. • Better performance and efficiency.
[61]	2023	To improve privacy and security through decentralized keying management, identity verification, and secure authentication.	Blockchain, and Cloud computing.	• Handles a large number of requests • Reliable message delivery. • Better performance regarding energy usage. • Minimal end-to-end latency.
[62]	2023	To achieve a secure, efficient, and reliable identity authentication.	Zero-knowledge proof technology, Blockchain, and Cloud computing.	• Security and controllability of user data. • Effective in avoiding security threats such as man-in-the-middle attacks. • Efficient authentication. • Short response time. • Low computational resource consumption.
[63]	2024	To create a distributed privacy-enhanced industrial data trading scheme.	Blockchain, and Cloud computing	• Feasible for sensitive data trading for multiple data owners. • Privacy-enhanced authentication and malicious user tracking.

Based on state-of-the-art solutions that integrate blockchain with cloud computing for identity management and authentication, the importance of combining these two technologies cannot be overstated. Blockchain technology offers effective identity management by efficiently mitigating both outsider and insider threats. Additionally, blockchain-based identity management and authentication systems significantly enhance security and privacy. Overall, these systems represent a substantial breakthrough in the field of identity management, with vast and important potential applications.

C. Blockchain for Improved Cloud Access Control

Access control involves regulating the actions that legitimate users are permitted to perform and monitoring each attempt to access system resources. The primary goal of an access control system is to safeguard the system resources from unauthorized or unwanted access by users [64]. The primary security and privacy concern associated with cloud computing is unauthorized access to private data. As a result of losing control over the data, , this type of access can be exploited by both internal and external hackers [65].

Consequently, the verification of cloud computing is crucial. Established verification mechanisms in the cloud build significant security threats. Perceptive data saved in the cloud can be settled through interference or illegal access by the cloud administrators and attackers. To protect the confidentiality

and integrity of the cloud-based data, this mentions the critical need for advanced access control technologies [66].

Blockchain can serve as a trustworthy solution for access control systems, removing the dependence on a single organization or entity within large-scale systems. Its decentralized and resilient architecture effectively overcomes the shortcomings of conventional access control methods, enabling the effective implementation of access control policies [64]. Therefore, integrating blockchain technology into cloud environments can lead to improved access control mechanisms [32,67].

In this section, various studies on the integration of blockchain technology in a cloud environment to improve access control mechanisms are presented and analyzed. Table 3 presents a synthesis of the studies' objectives, methodologies, and key strengths.

In the study by Wang *et al*. [68], the authors proposed a secure cloud storage framework that supports decentralized, fine-grained access management by combining the ciphertext-policy attribute-based encryption (CP-ABE) algorithm with blockchain-based access control. Data owner and user interactions are handled via Ethereum smart contracts, ensuring that each user's access is recorded on the Ethereum blockchain. The CP-ABE algorithm utilized an access tree to implement access control policies, allowing precise control over data access. The security analysis and experimental results indicate that the proposed scheme is both practical and successful.

According to Sohrabi *et al*. [69], the authors developed an access control model aimed at addressing the centralized security challenges in cloud storage. By leveraging smart contracts on a decentralized blockchain network, they were able to control access, mitigate cloud server vulnerabilities, and eliminate single points of failure. This decentralized approach strengthened data confidentiality and protected against unauthorized access.

Yang *et al*. [67] designed an access control framework named AuthPrivacyChain, focusing on privacy protection in cloud environments. All verification-linked compacts to the blockchain must be sent by the user. The composition was applied using the EOS, which is an enterprise operation system blockchain, within which the blockchain transactions access permission and related information are stored as additional data. The outcome of the trial accepted that only the verified operator cloud accessed the assets.

Gajmal and Udayakumar [70] imported a blockchain-based model for access control and data distribution in a dispersed cloud repository structure. The composition allows the secure allocation of secret keys to users and demonstrates access rules for scrambling distributed data. The system search service is equipped and measured using a smart contract on the Ethereum blockchain. Exploratory examination proved strong authentic user selection capabilities while fostering minimum response times.

Gao *et al*. [71] created an attribute-based browsable encryption algorithm that includes a multi-keyword explore service combined with the EOS blockchain platform to gain fine-grained access control. This system enables data owners to enforce detailed access policies, allowing only users with the attributes that meet the defined conditions to search and access accurate results. Experimental results and analysis demonstrated the practicality and effectiveness of the proposed solution.

The study conducted by Li [72] introduced a blockchain-driven verifiable access control mechanism for secure big data storage in cloud environments. A data exchange network built to combine blockchain technology and cloud computing was used to assess the strategy. The system could successfully detect and stop suspicious activity by utilizing blockchain components. It allowed medical institutions to share critical information without jeopardizing privacy while guaranteeing safe data transmission, management, and detection.

Sharma *et al.* [73] developed a blockchain architecture based on Java that incorporates user revocation and access control to ensure privacy in cloud storage systems. The solution made use of bilinear mapping-based encryption and CP-ABE for effective data access control and key generation. The blockchain system offered a safe and decentralized solution by distributing key management and user access regulations across data owners and attribute authorities. Comparisons and performance assessments showed that the suggested architecture outperformed current methods while preserving strong security and efficacy.

Xang *et al*. [74] presented a framework for cloud storage data access management based on blockchain technology, incorporating CP-ABE to improve security. The approach reduced the dependency on cloud servers for jobs that were outsourced by utilizing blockchain technology and smart contracts to guarantee data integrity and establish a decentralized verification process. To stop privacy leaks, a hidden access restriction was enforced using the CP-ABE algorithm. The investigation showed that the suggested plan successfully guaranteed data integrity within the cloud storage system in addition to increasing computational efficiency and achieving chosen ciphertext attack (CCA) protection.

Patel and Patel [75] proposed a system that uses blockchain technology to improve access control restrictions, strengthening the security of the cloud data storage. Smart contracts were added to the system to increase transparency and create a trust paradigm that eliminated the need for a middleman. Smart contracts and blockchain technology made it possible to securely handle data immutability, rejection, and file access. To manage user attributes, the system used an ABE scheme with various authorities, doing away with the necessity for a single authority. Additionally, the implementation of smart contracts decreased communication costs and the computational burden on consumers.

Yan *et al*. [76] developed a distributed access control system that allows fine-grained management by combining attribute-based searchable encryption with blockchain. To solve the trust and security concerns raised by third-party storage in conventional systems, the data ciphertext was kept in a distributed IPFS and the metadata ciphertext was safely distributed via blockchain smart contracts. To dynamically modify access rights, the smart contract also monitored user access behavior. According to the experimental data, the suggested system performs better than alternatives in terms of storage and processing efficiency.

Based on the study by Raghunandan *et al*. [77], the authors presented a solution that combines searchable attribute-based encryption (SABE) with blockchain technology to enable keyword searches on the blockchain and provide safe access to protected data. By using searchable encryption, the system allows users to safely access encrypted material without giving the cloud server important information. The blockchain stores encrypted keywords along with the storage addresses that relates to them. The results from the experiments undertaken showed that the suggested strategy provides significant efficiency gains.

Shahzad *et al*. [78], the authors proposed an algorithm that integrates blockchain, smart contracts, cloud computing, and CP-ABE to enable fine-grained access control and secure health data access. By harnessing the decentralization of blockchain alongside the scalability of cloud computing, the results showed that the proposed algorithm greatly boosted the effectiveness and safety of health data transfers.

Table 3: Blockchain-cloud integration for improved access control.

Source	Year	Research Goal	Used Techniques and Technologies	Strengths
[68]	2019	To provide fine-grained access control for the cloud.	CP-ABE, Blockchain and Cloud computing.	• Low cost for accessing files. • Solving the issue of a single point of failure caused by the center authority.
[69]	2020	To control access and mitigate threats to the cloud server through a decentralized solution.	Blockchain, and Cloud computing.	• Improved cloud data confidentiality. • Prevent illegal access to cloud data. • Reduced the single point of failure issue.
[67]	2020	To solve the problem of illegal access to resources by attackers of the cloud.	Blockchain, and Cloud computing.	• Prevent illegally access to resources by hackers and administrators. • Protect authorized privacy.
[70]	2021	To improve the security of data in the cloud through an access control mechanism.	Blockchain, and Cloud computing.	• Better genuine user detection rate. • Low responsiveness. • Effective in solving the single-point failure issue.

Table 3: Continued

[71]	2021	To achieve fine-grained access control through a fair and reliable blockchain-based searchable encryption scheme.	CP-ABE, Bloom filter, Blockchain, and Cloud computing.	• Feasible and practical. • Good performance.
[72]	2022	To apply classified access policies to secure cloud resources.	Blockchain, and Cloud computing.	• Acceptable level of security and privacy.
[73]	2022	To provide a fine-grained access control and robust user revocation in the cloud.	CP-ABE, Blockchain and Cloud computing.	• Efficient and scalable environment. • Privacy and confidentiality of the outsourced data.
[74]	2022	To establish a reliable access control mechanism in an untrusted cloud environment.	CP-ABE, Blockchain and Cloud computing.	• High computational efficiency. • Indistinguishability under the chosen ciphertext attacks.
[75]	2023	To provide enhanced access control policies for efficient cloud storage security.	Multi-Authority CP-ABE, Blockchain, and Cloud computing.	• Less computational and communication overhead. • Ownership management. • Security of data and logs. • Integrity verification.
[76]	2023	To achieve secure access to cloud data with low computational and trust costs.	Attribute-based searchable encryption, Blockchain and Cloud computing.	• High computing performance. • Data security and user access fairness. • Resistant to chosen plaintext attacks and keyword guessing attacks.
[77]	2023	To develop secure and efficient methods for managing sensitive data in decentralized systems.	SABE, Blockchain and Cloud computing.	• Provided data privacy. • Fine-grained access control. • Improved search capabilities. • Efficient revocation.
[78]	2024	To provide fine-grained access control for secure healthcare data management.	CP-ABE, Blockchain and Cloud computing.	• Enhanced the security of sensitive health data. • Efficient access for authorized users.

According to the in-depth review of the above solutions that integrated blockchain technology with cloud computing, most of the articles combined blockchain technology with CP-ABE or searchable attribute-based encryption. Existing solutions, such as CP-ABE and attribute-based encryption for cloud storage, still depend excessively on third-party entities, which presents serious security risks. In the field of access control, it is crucial to move away from relying on a trusted central authority to avoid potential vulnerabilities. To improve the performance and security of existing systems, integrating blockchain technology with cloud computing is necessary. By incorporating blockchain, the issue of a single point of failure caused by a central authority is addressed. The use of blockchain ensures that all access records are secure, immutable, and verifiable. With its decentralized and tamper-resistant nature, blockchain guarantees the security objectives including confidentiality, integrity, availability, authenticity, and the accountability of resources, while also protecting against unauthorized access and cyberattacks against cloud resources.

4.3 RQ3: What are the limitations of the Existing Solutions?

The main objective of this question is to emphasize the limitations that must be addressed in order to enhance the current solutions for improving the security of cloud environments.

A. Limitations of Blockchain for Enhancing Cloud Data Security in Rest and Transit

While blockchain offers valuable features such as immutability and decentralized trust, it presents several limitations when applied to securing cloud data at rest and in transit.

- Blockchain does not provide built-in data confidentiality, meaning sensitive data still requires external encryption mechanisms.
- Blockchain's immutability poses challenges when looking to modify or delete data to comply with regulations like the General Data Protection Regulation (GDPR).

- Key management complexity and a reliance on off-chain storage and encryption tools also reduce blockchain's effectiveness as a standalone solution.
- Finally, integrating blockchain into existing cloud architectures introduces a high technical overhead and interoperability challenges, making it more of a complementary technology than a primary solution for data protection in the cloud.

B. Limitations of Blockchain for Improved Cloud Identity Authentication and Management

Although blockchain introduces promising features for decentralized identity management and authentication in cloud computing, it comes with several significant limitations.

- One of the primary challenges is usability—most blockchain-based identity systems require users to manage private keys, which can be difficult to recover if lost and are impractical for mainstream adoption.
- Additionally, the lack of standardization across platforms hinders interoperability between different cloud services and identity frameworks.
- Furthermore, its immutability conflicts with regulatory requirements like GDPR, which mandates the ability to alter or delete personal data.
- Integrating blockchain with traditional identity systems introduces technical complexity and often requires hybrid solutions.

C. Limitations of Blockchain for Improved Cloud Access Control

While blockchain offers transparency and tamper-proof logging for access control in cloud environments, it faces several key limitations.

- Blockchain systems typically suffer from latency due to consensus mechanisms, making them unsuitable for the real-time access decisions required in dynamic cloud applications.
- Additionally, managing access control policies through smart contracts adds complexity, especially when permissions need to be frequently updated or revoked.
- The immutability of blockchain, while beneficial for auditability, becomes a drawback when flexible or time-sensitive access adjustments are necessary.
- Furthermore, integrating blockchain with existing centralized access control frameworks, presents technical and operational challenges.

These issues, combined with scalability constraints and the lack of standardized models for blockchain-based access control, suggest that while blockchain can enhance certain aspects of security, it is not yet a comprehensive solution for managing access in cloud environments.

4.4 RQ4: What are the Prospective Directions for Future Research in Leveraging Blockchain Technology to Enhance the Security of Cloud Computing Systems?

In light of the issues identified in the reviewed studies, the following points are proposed as potential avenues for future research into enhancing cloud security through blockchain technology:

- Future solutions must adopt hybrid architectures that combine blockchain with conventional security protocols.
- Advanced cryptographic frameworks—such as zero-knowledge proofs and homomorphic encryption - can further enhance privacy and data protection.
- Emphasis should be placed on building compliance-aware identity systems that align with regulatory frameworks like GDPR and testing security against emerging threats in distributed cloud environments.
- Emerging frameworks such as attribute-based access control powered by smart contracts offer promising alternatives to role-based models, enabling fine-grained control.
- Developing new consensus mechanisms that can improve scalability.
- Exploring the use of artificial intelligence and machine learning to enhance security and privacy through the integration of blockchain technology in a cloud environment.

5. Conclusions

In this article, an overview of cloud computing and blockchain technology is provided. The security aspects of integrating cloud computing with blockchain technology are then examined through analyzing various recent studies. Drawing on the most recent and relevant publications, this study presents an in-depth review of three core security domains in cloud computing and explores how blockchain integration can enhance them. While previous studies have typically focused on a single security domain, this review addresses three key areas: data security, identity authentication and management, and access control. In addition, this study identifies current limitations and outlines future research directions for leveraging blockchain to strengthen these security domains within cloud environments. According to the intensive review, the fusion of cloud computing and blockchain emerges as the most effective approach, offering enhanced security and decentralization. This combination improves authentication, authorization, data integrity, and privacy. It is essential to further explore this integration to support various sectors such as businesses, supply chains, healthcare, and industries. By doing so, it can deliver better data security, increased efficiency, and reduced costs.

Author contributions: Noor Ghazi M. Jameel: Conceptualization, Investigation, Methodology, Project administration, Resources and Writing – original draft. **Zryan Najat Rashid**: Conceptualization, Investigation, Methodology, Project administration, Resources and Writing – original draft. **Abdulkadir Şengür:** Conceptualization and Writing – review & editing.

Data availability: No data was used for the research described in this article.

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding: The authors did not receive support from any organization for the submitted work.

References

[1] D. Saadia, "Integration of cloud computing, big data, artificial intelligence, and internet of things: review and open research issues," *International Journal of Web-Based Learning and Teaching Technology*, vol. 16, no. 1, pp. 10–17, 2021, doi: 10.4018/IJWLTT.2021010102.

[2] I. Yaqoob, K. Salah, M. Uddin, R. Jayaraman, M. Omar, and M. Imran, "Blockchain for Digital Twins: Recent Advances and Future Research Challenges," *IEEE Network*, vol. 34, no. 5, pp. 290–298, 2020, doi: 10.1109/MNET.001.1900661.

[3] T. T. Huynh, T. D. Nguyen, and H. Tan, "A Survey on Security and Privacy Issues of Blockchain Technology," *International Conference on System Science and Engineering ICSSE 2019*, pp. 362–367, 2019, doi: 10.1109/ICSSE.2019.8823094.

[4] P. Jain, "Security Issues and their Solution in Cloud Computing," *International Journal of Computing & Business Research*, pp. 2229–6166, 2012.

[5] E. Worlanyo, "A Survey of Cloud Computing Security: Issues, Challenges and Solutions," *International Journal of Computer Science and Information Security*, vol. 14, no. 1, pp. 52–56, 2016, [Online]. Available: https://www.cse.wustl.edu/~jain/cse570-15/ftp/cld_sec/index.html

[6] P. Ravi Kumar, P. Herbert Raj, and P. Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," *Procedia Computer Science*, vol. 125, no. 2009, pp. 691–697, 2018, doi: 10.1016/j.procs.2017.12.089.

[7] L. Golightly, V. Chang, QA. Xu, X. Gao, and B. S. Liu, "Adoption of cloud computing as innovation in the organization," *International Journal of Engineering Business Management*, vol. 14, pp. 1–17, 2022, doi: 10.1177/18479790221093992.

[8] S. Nagadevi, P. Uma Maheswara Reddy, and V. Rama Krishna Reddy, "Load balancing in cloud computing using modified throtled algorithm," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11 Special Issue, pp. 1115–1119, 2019, doi: 10.35940/ijitee.K1226.09811S19.

[9] I. Zulifqar, S. Anayat, and I. Kharal, "A Review of Data Security Challenges and their Solutions in Cloud Computing," *International Journal of Information Engineering and Electronic Business*, vol. 13, no. 3, pp. 30–38, 2021, doi: 10.5815/ijieeb.2021.03.04.

[10] B. A. Alenizi, M. Humayun, and N. Z. Jhanjhi, "Security and Privacy Issues in Cloud Computing," *Journal of Physics Conference Series*, vol. 1979, no. 1, 2021, doi: 10.1088/1742-6596/1979/1/012038.

[11] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions, " *The Journal of Supercomputing*, vol. 76, no. 12, pp. 9493–9532, 2020, doi: 10.1007/s11227-020-03213-1.

[12] P. Vashisht, S. B. Bajaj, A. Jatain, and A. Narang, "Cloud Security: Challenges and Future Scope," *International Journal of Innovative Research in Engineering & Management*, vol. 10, no. 3, pp. 44–48, 2023, doi: 10.55524/ijirem.2023.10.3.8.

[13] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Computer Science*, vol. 48, no. C, pp. 204–209, 2015, doi: 10.1016/j.procs.2015.04.171.

[14] P. You, Y. Peng, W. Liu, and S. Xue, "Security issues and solutions in cloud computing," *32nd IEEE International Conference on Distributed Computing Systems Workshop ICDCSW 2012*, Macau, China, 2012, pp. 573–577, 2012, doi: 10.1109/ICDCSW.2012.20.

[15] M. Yang, " 68 Million Hashed Dropbox Passwords Dumped Online," 2016, [Online]. Available: https://www.pindrop.com/article/dropbox-passwords-dumped-online/.

[16] S. Khan, I. Kabanov, Y. Hua, and S. Madnick, "A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned," *ACM Transactions on Privacy and Security*, Vol. 26, No. 1, 2022, doi: 10.1145/3546068.

[17] M. Mendu, B. Krishna, S. Mohmmad, Y. Sharvani, and C. V. K. Reddy, "Secure Deployment of Decentralized Cloud in Blockchain Environment using Inter-Planetary File System," *IOP Conference Series Materials Science and Engineering*, vol. 981, no. 2, 2020, doi: 10.1088/1757-899X/981/2/022037.

[18] A. N. Misran, Syaifuddin, Muhammad and R. Khadafi, "A Meta-Analysis of Big Data Security : Using Blockchain for One Data Governance , Case Study of Local Tax Big Data in Indonesia," *Proceedings of the International Conference on Public Organization*, vol. 209, no. Iconpo 2021, pp. 198–206, 2022, doi: 10.2991/aebmr.k.220209.026.

[19] J. A. Malik, M. Zonain, and M. Akhter, "Empowering Cloud Security System With Blockchain Technology," *International Journal of Advanced Sciences and Computing*, vol. 2, no. 1, pp. 1–6, 2023.

[20] M. Ijaz Khan, M. Farhan, and S. Muhammad Ali Shah, "Exploring Benefits, Challenges and Security Considerations of Cloud Computing and Blockchain Technology to Enhance Healthcare Services," *Netherland International Journal of Applied Engineering Research*, vol. 7, no. 1, pp. 2666–2795, 2022.

[21] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 4, pp. 2521–2549, 2020, doi: 10.1109/COMST.2020.3020092.

[22] J. Doshi, "Applications of Blockchain Technology for Cloud Computing Security," *International Journal of Inovative Science and Reseach Technology*, vol. 7, no. 8, 2022, doi: 10.5281/ZENODO.7084189 .

[23] D. Yadav, A. Shinde, A. Nair, Y. Patil, and S. Kanchan, "Enhancing Data Security in Cloud Using Blockchain," *Proceeding of the International Conference on Intelligent Computing and Control Systems ICICCS*, Madurai, India, 2020, pp. 753–757, 2020, doi: 10.1109/ICICCS48265.2020.9121109.

[24] M. J. N. Sowmya, M. Srinivas, D. M. D. Reddy, M. V. V. Raju, and K. Chandran, "Blockchain-Enhanved Security Framework in Cloud Computing Integration," *International organization of Scientific Research*, vol. 14, no. 4, pp. 212–223, 2024

[25] K. Haripriya, N. C. Brintha, and C. K. Yogesh, "A survey on securing medical data in cloud using blockchain," *Advances in Parallel Computing*, vol. 39, pp. 279–287, 2021, doi: 10.3233/APC210150.

[26] M. Kasthuri, "Blockchain based Data Security as a Service in Cloud Platform Security," *International Journal on Cloud Computing Services and Architecture*, vol. 11, no. 6, pp. 1–8, 2021, doi: 10.5121/ijccsa.2021.11601.

[27] A. Yeboah-Ofori, S. K. Sadat, and I. Darvishi, "Blockchain Security Encryption to Preserve Data Privacy and Integrity in Cloud Environment," *Proceeding of International Conference on Future Internet of Things and Cloud (FiCloud)*, Marrakesh, Morocco, 2023, pp. 344–351, 2023, doi: 10.1109/FiCloud58648.2023.00057.

[28] R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooie, "An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain," *IEEE Access*, vol. 9, no. 1, pp. 69513–69526, 2021, doi: 10.1109/ACCESS.2021.3077123.

[29] S. Sudha and S. S. Manikandasaran, "Cloud Data Security Using Cryptoga and Blockchain Recovery," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 16, pp. 6286–6300, 2023.

[30] P. K. Kollul, M. Saxena, K. Phasinam, T. Kassanuk, and M. Mustafa, "Blockchain Techniques for Secure Storage of Data in Cloud Environment," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 11, pp. 1515–1522, 2021, doi: 10.17762/turcomat.v12i11.6074.

[31] I. Abrar and J. A. Sheikh, "Current trends of blockchain technology: architecture, applications, challenges, and opportunities," *Discover Internet of Things*, vol. 4, no. 1, 2024, doi: 10.1007/s43926-024-00058-5.

[32] A. Khanna, A. Sah, V. Bolshev, A. Burgio, and V. Panchenko, and M. Jasiński, "Blockchain–Cloud Integration: A Survey," *Sensors*, vol. 22, no. 14, 2022, doi: 10.3390/s22145238 2022.

[33] I. Hamid and M. Frikha, "Blockchain-Enhanced Cybersecurity and Privacy in Cloud Computing: a Systematic Literature Review," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 2, pp. 514–531, 2024.

[34] H. M. Rai, K. K. Shukla, L. Tightiz, and S. Padmanaban, "Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies," *Heliyon*, vol. 10, no. 19, p. e38917, 2024, doi: 10.1016/j.heliyon.2024.e38917.

[35] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Ostrava, Czech Republic, 2018, doi: 10.1109/HealthCom.2018.8531125.

[36] D. M. K. Bader, "Blockchain-based Security Measure for Cloud-based Healthcare System,"*International Journal on*

Emerging Technologies, vol. 11, no. 5, pp. 672–679, 2020.

[37] K. Meenakshi, "An Efficient Security System For Cloud Servers Using Blockchain Technique," Ph.D. thesis, Department of Engineering, Saveetha University, India, 2022. http://hdl.handle.net/10603/429365.

[38] R. K. Motupalli, and K. Prasad K, "Augmenting The Cloud Environment Security Through Blockchain Based Hash Algorithms," *Journal of Computer Sciences Institute*, vol. 26, no. November 2022, pp. 1–6, 2023, doi: 10.35784/jcsi.3064.

[39] A. Amanat, M. Rizwan, C. Maple, Y. Bin Zikria, A. S. Almadhor, and S. W. Kim, "Blockchain and cloud computing-based secure electronic healthcare records storage and sharing," *Frontiers in Public Health*, vol. 10, 2022, doi: 10.3389/fpubh.2022.938707.

[40] D. Rani, N. S. Gill, and P. Gulia, "Design of a Cloud-Blockchain-based Secure Internet of Things Architecture," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, pp. 443–454, 2022, doi: 10.14569/IJACSA.2022.0130851.

[41] S. Gousteris, Y. C. Stamatiou, C. Halkiopoulos, H. Antonopoulou, and N. Kostopoulos, "Secure Distributed Cloud Storage based on the Blockchain Technology and Smart Contracts," *Emerging Science Journal*, vol. 7, no. 2, pp. 469–479, 2023, doi: 10.28991/ESJ-2023-07-02-012.

[42] C. Gou and X. Deng, "A blockchain-based security model for cloud accounting data," *International Journal of Ambient Computing and Intelligenc*, vol. 14, no. 1, pp. 1–16, 2023, doi: 10.4018/IJACI.332860.

[43] A. E. N. Saah, J. J. Yee, and J. H. Choi, "Securing Construction Workers' Data Security and Privacy with Blockchain Technology," *Applied Sciences*, vol. 13, no. 24, 2023, doi: 10.3390/app132413339.

[44] M. Abubakar, I. Ame, T. Mangai, and F. Al-Turjman, "Ethereum Blockchain, AI, and Cloud storage for Medical Reports," *Multidisciplinary Advance Sciences and Technology*, vol. 2, no. 2, 2023.

[45] G. Shrivastava and S. Patel, "Secure Storage and Data Sharing Scheme Using Private Blockchain-Based HDFS Data Storage for Cloud Computing," *International Journal of Computer Networks and Applications*, vol. 10, no. 1, pp. 28–38, 2023, doi: 10.22247/ijcna/2023/218509.

[46] M. Rashmi, R. Goenka, R. S. Tenginkai, and V. Singh, "Cloud Storage and Retrieval Using Blockchain," *International Research Journal of Engineering and Technology*, pp. 317–321, 2023, [Online]. Available: www.irjet.net.

[47] A. Gund, P. Mahadik, A. R. Thorat, and G. K. Yevle, "Data De-Duplication Using Blockchain with Advanced Security in Cloud Computing," *SSRN Electronic Journal*, 2022, doi: 10.2139/ssrn.4289505.

[48] X. Guo, G. Liang, J. Liu, and X. Chen, "Blockchain-Based Cognitive Computing Model for Data Security on a Cloud Platform," *Computers Materials and Continua*, vol. 77, no. 3, pp. 3305–3323, 2023, doi: 10.32604/cmc.2023.044529.

[49] S. J. Rajawat, M. Kaushik, and S. Kumar Yadav, "Cloud Enabled e-Banking Payment Security Implementation using Blockchain Technology," *Journal of Electrical Systems*, vol. 20, no. 7s, pp. 1445–1455, 2024, doi: 10.52783/jes.3715.

[50] J. Huang and J. Yi, "The key security management scheme of cloud storage based on blockchain and digital twins," *Journal of Cloud Computing*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-023-00587-4.

[51] A. B. Kathole, K. Netaji Vhatkar, A. Goyal, S. Kaushik, A. Sanjiv Mirge, P. Jain, M. S. Soliman, and M. Tariqul Islam, "Secure Federated Cloud Storage Protection Strategy Using Hybrid Heuristic Attribute-Based Encryption With Permissioned Blockchain," *IEEE Access*, vol. 12, no. September, pp. 117154–117169, 2024, doi: 10.1109/ACCESS.2024.3447829.

[52] J. Li, "A review of identity authentication based on blockchain technology," *Applied and Computational Engineering*, vol. 30, no. 1, pp. 173–178, 2024, doi: 10.54254/2755-2721/30/20230094.

[53] A. M. Mostafa, E. Rushdy, R. Medhat, and A. Hanafi, "An identity management scheme for cloud computing Review, challenges, and future directions, " *Computer Systems Science and Engineering*, vol. 43, no. 3, pp. 967–984, 2022, doi: 10.32604/csse.2022.024854.

[54] A. Alsirhani, M. Ezz, and A. M. Mostafa, "Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing," *Computer Systems Science and Engineering*, vol. 43, no. 3, pp. 967–984, 2022, doi: 10.32604/csse.2022.024854.

[55] H. Khanna, G. Gupta, and H. Sharma, "Investigating Identity Management and Authentication Solutions Using Blockchain Technology," *SSRN Electronic Journal*, pp. 1–10, 2024, doi: 10.2139/ssrn.4922025.

[56] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management," *Proceeding of IEEE 16th International Conference Dependable, Autonomic. Secure Computing, IEEE 16th International Conference on Pervasive Intelligence Computing, IEEE 4th International Conference on Big Data Intelligence and Computing and CyberScience and Technology*, Athens, Greece, 2018, pp. 716–723, doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126.

[57] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, "Authentication protocol for cloud databases using blockchain mechanism," *Sensors (Switzerland)*, vol. 19, no. 20, pp. 1–13, 2019, doi: 10.3390/s19204444.

[58] S. Wang, R. Pei, and Y. Zhang, "EIDM: A Ethereum-Based Cloud User Identity Management Protocol," *IEEE Access*, vol. 7, pp. 115281–115291, 2019, doi: 10.1109/ACCESS.2019.2933989.

[59] V. R. Kebande, F. M. Awaysheh, R. A. Ikuesan, S. A. Alawadi, and M. D. Alshehri, "A blockchain-based multi-factor

authentication model for a cloud-enabled internet of vehicles," *Sensors*, vol. 21, no. 18, pp. 1–20, 2021, doi: 10.3390/s21186018.

[60] M. Vivekanandan, V. N. Sastry, and U. Srinivasulu Reddy, "Blockchain based Privacy Preserving User Authentication Protocol for Distributed Mobile Cloud Environment," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1572–1595, 2021, doi: 10.1007/s12083-020-01065-3.

[61] S. N. Prasad and C. Rekha, "Block chain based IAS protocol to enhance security and privacy in cloud computing," *Measurement Sensors*, vol. 28, no. August, p. 100813, 2023, doi: 10.1016/j.measen.2023.100813.

[62] Z. Du, W. Jiang, C. Tian, X. Rong, and Y. She, "Blockchain-Based Authentication Protocol Design from a Cloud Computing Perspective," *Electronics*, vol. 12, no. 9, 2023, doi: 10.3390/electronics12092140.

[63] J. Fang, T. Feng, X. Guo, R. Ma, and Y. Lu, "Blockchain-cloud privacy-enhanced distributed industrial data trading based on verifiable credentials," *Journal of Cloud Computing*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-023-00530-7.

[64] V. C. Hu, "Blockchain for Access Control Systems," 2022, doi: 10.6028/NIST.IR.8403. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8403.pdf.

[65] P. M. Tehrani, G. Kotsis, and A. R. Pranata, "Blockchain Technology for Addressing Privacy and Security Issues in Cloud Computing," *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, pp. 194–200, 2022, doi: 10.34190/iccws.17.1.41.

[66] S. Liu, "Towards Secure Blockchain-enabled Cloud Computing: A Taxonomy of Security Issues and Recent Advances," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 8, pp. 917–926, 2023, doi: 10.14569/IJACSA.2023.01408101.

[67] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[68] S. Wang, X. Wang, and Y. Zhang, "A Secure Cloud Storage Framework with Access Control Based on Blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019, doi: 10.1109/ACCESS.2019.2929205.

[69] N. Sohrabi, X. Yi, Z. Tari, and I. Khalil, "BACC Blockchain-Based Access Control For Cloud Data," *Proceedings of the Australasian Computer Science Week Multiconference*, no. 10, pp. 1–10, 2020, doi:10.1145/3373017.3373027.

[70] Y. M. Gajmal and R. Udayakumar, "Blockchain-Based Access Control and Data Sharing Mechanism in Cloud Decentralized Storage System," *Journal of Web Engineering*, vol. 20, no. 5, pp. 1359–1388, 2021, doi: 10.13052/jwe1540-9589.2054.

[71] H. Gao, S. Luo, Z. Ma, X. Yan, and Y. Xu, "BFR-SE: A Blockchain-Based Fair and Reliable Searchable Encryption Scheme for IoT with Fine-Grained Access Control in Cloud Environment," *Wireless Communications and Mobile Computing*, vol. 2021, 2021, doi: 10.1155/2021/5340116.

[72] X. Li, "A Blockchain-Based Verifiable User Data Access Control Policy for Secured Cloud Data Storage," *Computational Intelligence and Neuroscience*, 2022, doi:10.1155/2022/2254411.

[73] P. Sharma, R. Jindal, and M. Dutta Borah, "Blockchain-based cloud storage system with CP-ABE-based access control and revocation process," *The Journal of Supercomputing*, vol. 78, no. 8, pp. 7700–7728, 2022, doi:10.1007/s11227-021-04179-4. .

[74] X. Yang, A. Chen, Z. Wang, and S. Li, "Cloud Storage Data Access Control Scheme Based on Blockchain and Attribute-Based Encryption," *Security and Communication Networks*, vol. 2022, 2022, doi: 10.1155/2022/2204832.

[75] P. Patel and H. Patel, "Achieving A Secure Cloud Storage Mechanism Using Blockchain Technology," *International Journal of Computer Theory and Engineering*, vol. 15, no. 3, pp. 130–142, 2023, doi: 10.7763/IJCTE.2023.V15.1342.

[76] L. Yan, L. Ge, Z. Wang, G. Zhang, J. Xu, and Z. Hu, "Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment," *Journal of Cloud Computing*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-023-00444-4.

[77] K. R. Raghunandan, B. Kallapu, R. Dodmane, N. S. Krishnaraj Rao, S. Thota, and A. K. Sahu, "Enhancing Cloud Communication Security: A Blockchain-Powered Framework with Attribute-Aware Encryption," *Electronics*, vol. 12, no. 18, 2023, doi: 10.3390/electronics12183890.

[78] A. Shahzad, W. Chen, M. Shaheen, Y. Zhang, and F. Ahmad, "A robust algorithm for authenticated health data access via blockchain and cloud computing," *PLoS One*, vol. 19, no. 9, pp. 1–25, Sept. 2024, doi: 10.1371/journal.pone.0307039.