PUNIA, A., GULIA, P., GILL, N.S., IBEKE, E., IWENDI, C. and SHUKLA, P.K. 2024. A systematic review on blockchain-based access control systems in cloud environment. *Journal of cloud computing* [online], 13, article number 146. Available from: https://doi.org/10.1186/s13677-024-00697-7

A systematic review on blockchain-based access control systems in cloud environment.

PUNIA, A., GULIA, P., GILL, N.S., IBEKE, E., IWENDI, C. and SHUKLA, P.K.

2024

© The Author(s) 2024.

OpenAIR @RGU

This document was downloaded from https://openair.rgu.ac.uk

CC BY

Punia *et al. Journal of Cloud Computing* (2024) 13:146
https://doi.org/10.1186/s13677-024-00697-7

Journal of Cloud Computing

REVIEW Open Access

A systematic review on blockchain-based access control systems in cloud environment

Aarti Punia[1], Preeti Gulia[1], Nasib Singh Gill[1], Ebuka Ibeke[2*], Celestine Iwendi[3*] and Piyush Kumar Shukla[4]

Abstract
The widespread adoption of cloud computing has dramatically altered how data is stored, processed, and accessed in an era. The rapid development of digital technologies characterizes all this. The widespread adoption of cloud services has introduced new obstacles to guaranteeing secure and expeditious access to sensitive data. Organizations of all types find user-friendly and cost-effective solutions crucial, which is why they consider cloud services essential. The availability of the cloud hampers access control security in systems that are constantly and remotely changing. Conventional methods of access control are efficient, but the advanced world of technology exposes them to more threats. Applying blockchain technology to cloud access control systems, which are decentralized, transparent, and tamper-proof, has overcome these challenges. This paper aims to discuss the potential of blockchain in enhancing access management, security and trust in cloud computing. Besides, this scholarly article reviews the evolving area of blockchain-based access control systems and synthesizes the findings of 118 selected papers from various academic repositories. Based on this systematic review of the studies, twelve different types of blockchain-based access control paradigms can be identified. This work provides a critical analysis of the research on blockchain technology in access control systems, with a focus on scalability, compatibility, and security challenges. It also highlights areas that require further research and proposes directions for future research to advance this rapidly growing area of scholarship.

Keywords Blockchain, Access control system, Cloud computing, Security, Trust, Systematic review

Introduction

Cloud computing has caused a paradigm shift that can be described as an era of unprecedented convenience and expansion in the area of information technology. Businesses around the world leverage cloud solutions and services to enhance efficiency, cut costs, and promote collaboration. However, the fast adoption of cloud technology has introduced advanced security questions on governing and securing information [1]. Traditional methods of access control in the cloud computing model have always been used to effectively regulate user permissions, safeguard data and meet compliance standards. Generally, such systems rely on centralized means of identifying users and granting them access to the resources located in the cloud, which could include username/password or digital certificates [2]. Hybrid cryptography access control solutions can facilitate secure cloud storage and exchange of healthcare information. Steganography-based access control systems can also be used to tackle problems related to key sharing and secure data

*Correspondence:
Ebuka Ibeke
e.ibeke@rgu.ac.uk
Celestine Iwendi
c.iwendi@bolton.ac.uk
[1]Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India
[2]School of Computing, Engineering & Technology, Robert Gordon University, Aberdeen, UK
[3]School of Creative Technologies, University of Bolton, Bolton, UK
[4]Computer Science & Engineering Department, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya (Technological University of Madhya Pradesh), Bhopal, India

Springer Open

© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

transfer in healthcare applications [3]. Despite these conventional techniques showing positive results in many cases, they are not beyond their share of disadvantages. A big disadvantage of traditional access control systems is their vulnerability to the central points and single points of attack. Hackers always consider authentication servers or identity providers when they intend to gain unauthorized access to sensitive data or other valuable assets [4]. A multilabel-based scalable access control system for cloud services such as IaaS, PaaS, and SaaS may be provided. This access control service is managed by a reliable access control provider, which is an outside party [5, 6]. While the penetration of centralized systems is still a topic of discussion, if these systems are penetrated then firms may face disastrous results in terms of leakage of data, financial losses and reputation loss. Furthermore, the tradition access control mechanisms are frequently not very clear and there is no way of keeping a record of the activity of the users, which is a problem for enterprises in terms of control of access. Storing sensitive data on remote servers that are managed by third-party providers can be unsafe, as it introduces potential vulnerabilities. Recent high-profile cases have raised concerns about data leaks and unauthorized cloud access. One cloud-based analytics and data storage company, Snowflake, for instance, was involved in a cybersecurity scandal. Ticketmaster and Santander Bank were among the well-known customers whose sensitive data was stolen due to unauthorized access to their systems [7]. In the Trello Data Scraping case, the attackers scraped data from 15 million Trello users and posted it on the dark web [8]. The data of about 57,000 Bank of America customers was exposed in the Bank of America Ransomware attack [9].

Cloud services are centralized. Therefore, a CSP's infrastructure vulnerability could harm many consumers at once. Control and ownership issues are another problem [10]. Users must trust the CSP for cloud data and application maintenance, administration, and availability [11]. This reliance can cause issues if the provider goes down. Various countries have various data storage and access policies, raising worries about data sovereignty and compliance. This can hinder multinational businesses. Subsequently, cloud services can grow expensive over time, especially for enterprises with significant data storage and processing needs, negating initial cost advantages. Owing to these disadvantages, there has been a rise in interest in substitute alternatives, with blockchain technology emerging as a compelling choice to address several problems. The underlying technology that powers cryptocurrencies like Ethereum and Bitcoin is called blockchain. It ensures that transactions across a network of nodes are recorded in a decentralized, immutable ledger that is impossible to tamper with. Organizations can eliminate the requirement for centralized authentication servers by utilizing blockchain technology to decentralize access control mechanisms.

Access control policies and permissions can be implemented with smart contracts, which are self-executing codes published on a blockchain network. These contracts automatically enforce access rules according to established conditions and criteria [12]. One advantage of access control solutions based on the blockchain is their anti-fragility against single points of failure and adversarial manipulations. Since the access control policies are in a distributed ledger, which stores and executes them, the attackers do not have a single point of attack. The access control system remains functional and guarantees the preservation of resources, which are available and secured at any given time, despite the failure or malicious activities of certain nodes and components. Challenges that organizations may encounter include the ability to detect security threats, compliance with set norms, and sanctions against individuals who breach laws on access to certain resources. This is only if they have no adequate audit trail [6]. To address these challenges, organizations are gradually considering integrating blockchain technology into cloud-based access control systems to increase security, flexibility, and efficiency. Several challenges are linked with cloud computing and these are; security and privacy. Nowadays, solutions based on the blockchain are applied in various spheres for practical usage in the field of access control. The use of blockchain technology in the healthcare industry protects electronic health records (EHR) as only the relevant personnel in the healthcare industry can access the information [13]. Thus, the most suitable solution for healthcare operations' requirements and variety of needs, as well as the most stringent data security and patient privacy requirements, would be a combination of using blockchain technology with traditional access control models. It enhances data security, privacy, and meaningful use of information by integrating with cloud-based EHR platforms to facilitate data exchange [14].

It is also evident that blockchain-based access control systems play the role of protecting digital assets, enabling safe transactions, and denying access to financial data. Connecting with cloud-based financial platforms enhances security, auditability, and productivity and minimizes risks such as fraud and hacking [15]. In the future, the integration of blockchain into cloud-based access control systems can be a promising area that will contribute to the development of new ideas and ideas regarding procedures related to the management of digital identities. Decentralized identity and verifiable credentials offer individuals more control over their identity data and decrease reliance on traditional forms of authentication. Blockchain integration with cloud-based access control ensures a significant evolution of how enterprises manage user permissions, secure information, and ensure compliance. These are the best solutions to the existing

centralized authentication issues since blockchain systems can decentralize access control while increasing transparency and the safety of transactions. An innovative method of fair trading that can be achieved through smart contracts is the absence of a trustworthy third party, and a verifiable data integrity system can be implemented to guarantee data accuracy [16]. While the trend of adopting blockchain technology in enterprises continues to grow, cloud-based access control appears to be decentralized, transparent, and secure in the future. This study seeks to answer the following questions:

- What problems exist with the access control systems in use today?
- How does blockchain overcome these issues?
- What are the challenges in building a blockchain-based access control system?
- What are the gaps in the related research?

Motivation

The rationale for this analysis of frameworks for access control based on blockchain is the requirement of secure, decentralized solutions in a world that is integrating more and more. Since the access control systems are centralized, they can be hacked, possess single points of failure, and be inconvenient for the management of permits across numerous systems. Blockchain's decentralization, immutability, and transparency make it a promising alternative for access control security and trust. The review's main goal is to investigate how blockchain's decentralized and unchangeable structure may be used to solve the security and privacy issues that come with using conventional cloud access control approaches. This research systematically reviews blockchain-based access control frameworks to identify current trends, difficulties, and best practices to help design more secure, scalable, and efficient systems. This review will also assist in identifying gaps in the existing literature and will suggest possibilities for future research. This will ultimately contribute to the development of more secure digital infrastructures.

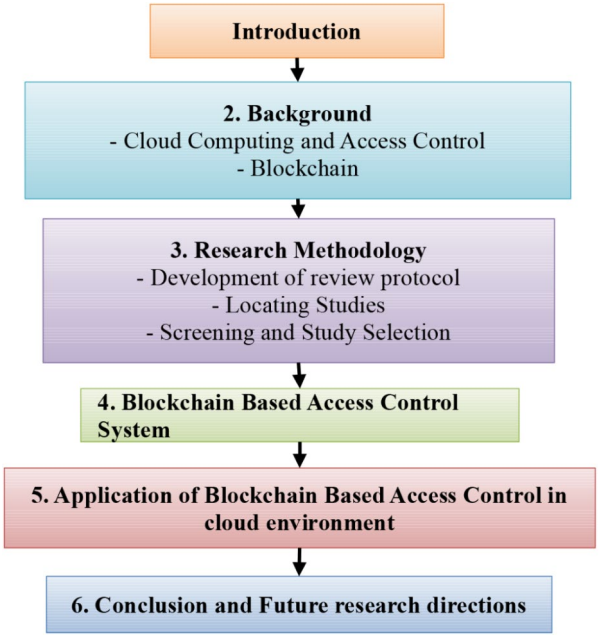

Fig. 1 Structure of the study

The layout of the paper is defined in Fig. 1; after the discussion of the introduction of the topic, a thorough knowledge of cloud computing, especially about the access control mechanism, is discussed, and then blockchain is discussed. The research approach used for the literature review, including the inclusion and exclusion criteria, is covered in the third section. In the fourth section, blockchain-based access control is thoroughly discussed, and it is classified into 12 different categories. The literature is grouped according to their respective subcategories. In the fifth section, applications of blockchain-based access control specific to cloud computing are explained. The sixth section discusses the future research direction along with the conclusion.

Related works

We examine recent advancements in blockchain-based access control in this section. Performance optimization, security, and blockchain integration with technologies are addressed in numerous research and applications. Routh and Ranjan [17] Extensively analyse three traditional and seven hybrid cloud computing access control systems, emphasizing the relevance of granularity in model selection and demonstrating the benefits of fine-grained access control mechanisms. Patil et al. [18] investigates many blockchain-based techniques that have been suggested in the literature to manage IoT device access and enhance privacy and security in the supply chain, Vehicular Ad-Hoc Network (VANET), and healthcare networks. Butun and Osterberg [19] examine peer-to-peer (P2P) network access control schemes and propose a threshold signature-based authentication system, trusted computing and reputation-based authorization systems, and Certificate Revocation List (CRL) with group signatures to revoke permission from blockchain systems. Wijesekara [20] explores blockchain-based access control in networking to ensure that only authorized devices complete defined operations to prevent malicious activity. The author classifies various access control techniques into four proposals and evaluates them based on blockchain roles, access control methodologies, network aspects, and other criteria. Sharma et al. [21] study the use of blockchain technology to secure cloud storage, motivated by the increasing demand and importance of

blockchain innovation in addressing recent technological issues. Praharaj et al. [22] review the literature to identify and evaluate cloud access control requirements and techniques, answering research questions on security models, proposed mechanisms, and their pros and cons to help researchers and practitioners evaluate existing models and identify gaps. Li et al. [10] offered a cloud-edge hybrid trust management framework with a double-blockchain transaction model. They also provided a taxonomy and evaluation of blockchain-based trust management techniques in cloud computing, as well as analyzed and compared them. They also made suggestions for future research and problems. Our systematic review examines how blockchain technology can improve cloud access control. We grouped suggested papers into 12 different groups and then analyzed them.

Background

We will go over the various cloud computing access methods in this section. Businesses can determine which access control strategy is most appropriate for them by comparing several strategies. After that, the basics of blockchain technology are discussed.

Cloud computing and access control

Cloud computing is distinguished by its ability to provide computer resources over the internet as and when needed. The transition from traditional on-premises infrastructure to cloud-based solutions has greatly changed the way firms handle their IT requirements. Although the advantages of cloud resources are significant, including cost-effectiveness and scalability, the fact that they are shared and accessed remotely brings about new and unique security challenges [22]. Access control is an essential element of a security strategy, which regulates the permissions for individuals to access specific resources within a system. Cloud settings provide problems to standard access control approaches due to issues such as centralization, single points of failure, and susceptibility to illegal access [23]. These difficulties need a reassessment of current access control frameworks, leading to the investigation of novel solutions like blockchain.

Access control models provide the techniques and regulations employed to oversee and limit access to information or resources, as depicted in Fig. 2. There are five well-known models of cloud computing access control:

Role-based access control (RBAC)

This streamlines access management by allocating permissions to roles designated by an organization rather than individuals, as shown in Fig. 2. Users are categorized based on their work responsibilities and assigned rights that are relevant to their roles [24]. Users automatically receive permissions for the roles they are assigned to, making the management of access control more efficient, as shown in Fig. 3. This technique improves security by reducing human error and streamlining the process of adding and removing users. When users require dynamic permissions, the level of flexibility may be limited.

Attribute-based access control (ABAC)

This involves the use of user attributes, resources, and environment to determine access. Such attributes can include user roles, time of access, location, and other contextual data that might be useful. ABAC allows administrators to define complex access control policies because the decision process is not only based on a set of parameters but also takes into consideration the multiple values of each parameter in a detailed manner as shown in Fig. 4 [25]. This methodology allows access policies that are aware of the context, and that is why this approach is effective to use in different environments with various access requirements. The overall coordination and supervision of a range of diverse attributes and regulations is challenging.

Mandatory access control (MAC)

This kind of access control technique is mostly applicable in environments that require extra security, for instance, military and government networks. Its methodical and applicative approach marks this paradigm. The MAC systems constrain access decisions through a central authority, as demonstrated in Fig. 5. The decisions are based on the security labels and categorization levels that may be

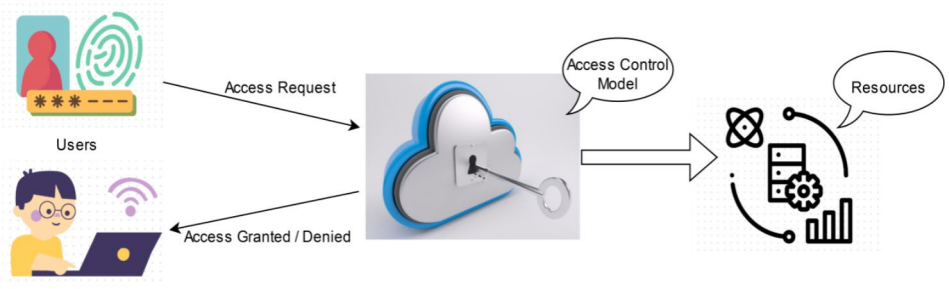

Fig. 2 Access control mechanism

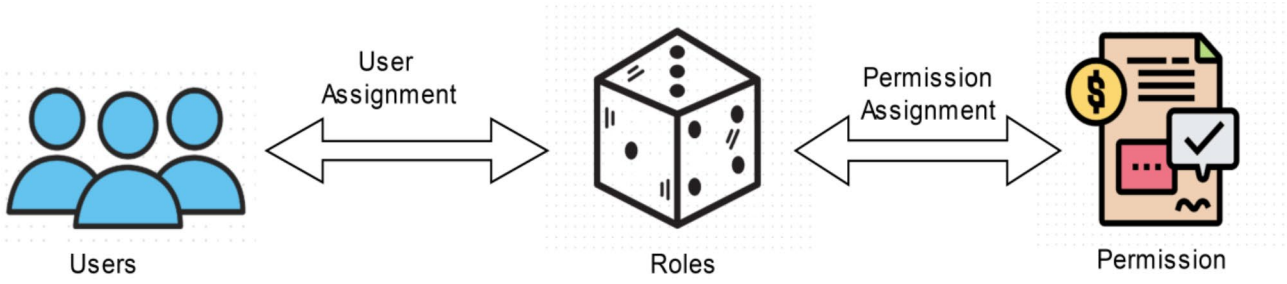

Fig. 3 The overview of role-based access control

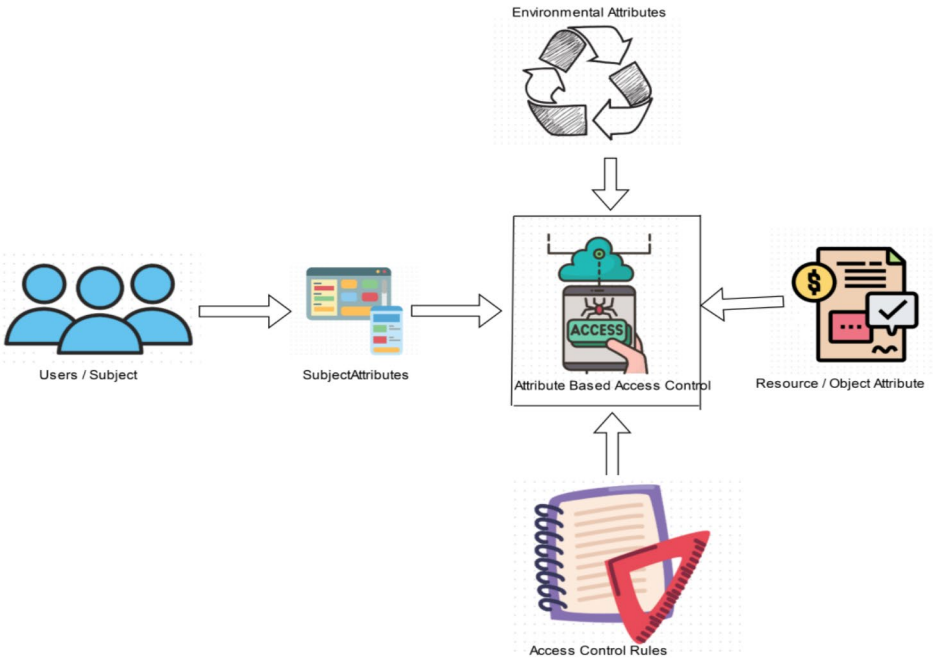

Fig. 4 Attribute based access control

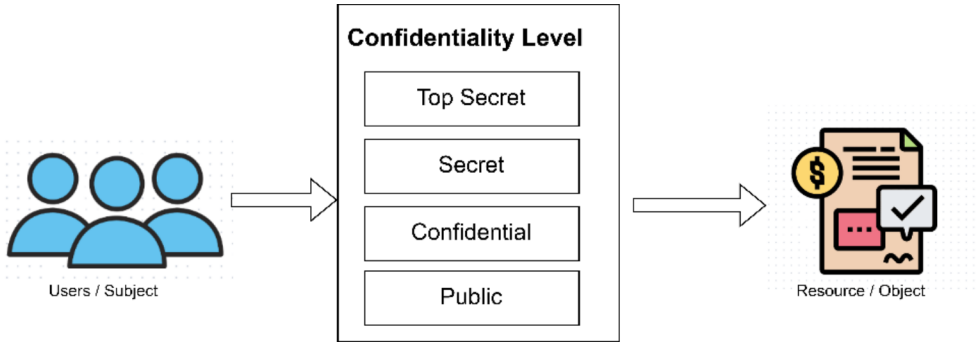

Fig. 5 Mandatory access control

assigned to the users and the resources [26]. Users are unable to modify the policies, that make sure the preservation of data confidentiality and integrity. Establishing MAC in dynamic contexts with flexible access control might be challenging, but it is highly successful in securing sensitive data.

Discretionary access control (DAC)

Resource owners decide who may access content under discretionary access control. In DAC, a resource is allocated to an owner who has the autonomy to independently grant or refuse access privileges to other users, as shown in Fig. 6. Through this decentralized approach,

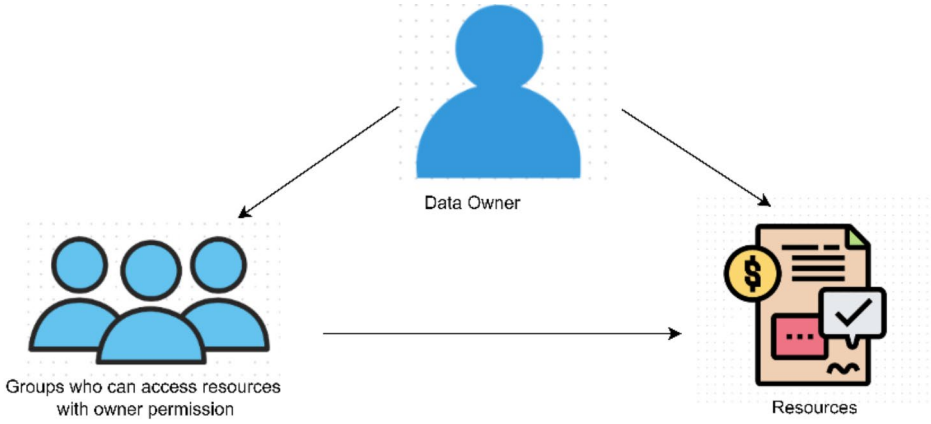

Fig. 6 Discretionary access control

Table 1 Different access control methods in cloud environment

Criteria	RBAC [28]	ABAC [29]	DAC [30]	MAC [31]	ReBAC [32]
Definition	Enables access according to a person's position within an organization	Gives access according to qualities (or traits) rather than responsibilities to decide access.	Gives a person total control over all they possess	End users do not influence privileges; access control is managed solely by the system owner.	Roles are dynamically assigned to users according to the owner's or system administrator's stated criteria.
Core Concept	Roles	Attributes	Ownership and Permissions	Labels and Policies	Rules
Granularity	Coarse	Fine	Medium	Fine	Fine
Permission Assignment	Role-based	Attribute-based	Owner-based	Policy-based	Rule-based
Flexibility	Limited	High	Moderate	High	High
Scalability	Good	Good	May become complex	May become complex	Good
Complexity	Low	Moderate	Moderate	High	Moderate
Use Cases	Enterprise Systems	Dynamic Environments	File Systems, Database Systems	Military, Government	Highly Customized Environments
Example	Assigning roles like Admin, User	Defining access based on attributes	Assigning permissions to owners	Classifying information	Defining rules for specific cases

users can regulate the right to use their resources, enhancing flexibility [17]. Resource owners may not consistently implement access controls, leading to inconsistent security measures. DAC is employed in less regulated settings with permissive access control.

Rule-based access control (ReBAC)

This also known as Relationship-Based Access Control, determines access decisions based on the relationships between users and resources. Access control policies analyze the linkages and interactions between entities in a system. Conditional expressions are utilized to articulate intricate access conditions in these regulations [27]. ReBAC allows for precise access control permissions thanks to the dynamic nature of organizational linkages. Creating and overseeing a comprehensive set of regulations can be challenging and may necessitate meticulous examination to prevent unforeseen outcomes.

Different access control methods are explained in Table 1, showing a comparative evaluation of all five access control techniques based on the specific parameters. RBAC is used to grant access based on a person's role in an organization and has a rigid permission assignment model with moderate flexibility, good scalability, and low complexity. ABAC grants access based on attributes or characteristics of the subject, which results in high flexibility and the ability to achieve high granularity. DAC enables people to have control over their assets and it is moderately flexible and complex since it is based on owner permissions. The MAC is managed only by the system owner with high flexibility and fine granularity but high complexity suitable for the military and government. ReBAC is configured in a way that it assigns roles based on certain policies, it has high flexibility, good scalability and moderate complexity which is suitable for a highly dynamic environment. There are specific applications for each: enterprise systems for RBAC, dynamic environments for ABAC, file systems for DAC and classifying information for MAC.

Table 2 shows the merits and demerits of all access control mechanisms. One organization or enterprise can choose according to its needs and keep in account its merits and disadvantages. RBAC makes administration easier by associating responsibilities with users, however, it is not very flexible and lacks detailed control. High flexibility is provided by ABAC together with the ability to manage different policies in complex environments, however, ABAC is rather sensitive to infrastructure and may be rather difficult to manage. MAC provides high confidentiality and centralized control that is desirable in secure networks but it is rigid and can cause high overhead. The advantages of DAC are that it is simple to use and easy to administrate, especially in data-sharing scenarios, yet it is less secure and results in the creation of insecure policies. ReBAC offers real-time, context-aware access control decisions and improves security using precise rules; however, the rules administration is challenging and requires significant resources.

Blockchain

The idea of trust in data transfers has undergone a fundamental transformation because of blockchain technology [33]. At its core, blockchain is a decentralized ledger that records transactions across a network of computers in a safe, transparent, and unchangeable manner. Although this technology is the backbone of cryptocurrencies like Bitcoin, it has applications in banking, supply chain management, healthcare, and other fields in addition to digital money. As shown in Fig. 7, which depicts the fundamental architecture of blockchain, one of the most notable characteristics of blockchain is its decentralized nature. Blockchain, in contrast to conventional centralized databases, disperses its ledger among numerous nodes. It guarantees that no single entity possesses authority over the entire network [34]. The decentralization of data reduces the likelihood of data tampering and cyber-attacks, as modifying data on one node would need simultaneous modifications on the majority of nodes in the network.

The immutability of blockchain is a crucial characteristic. A transaction cannot be changed or withdrawn after it has been recorded on the blockchain. This is accomplished through the use of cryptographic hashing, which is a procedure that transforms data into a distinct sequence of characters. Every block includes a cryptographic hash of the preceding block, resulting in a chain that is mathematically interconnected [35]. Modifying any block would result in a modification of its hash value, causing a mismatch with the subsequent blocks. This would provide clear evidence of tampering. One well-known use of blockchain technology is smart contracts. The terms of these autonomous contracts are explicitly programmed into the software. They autonomously enforce and execute the contracts after pre-established circumstances are fulfilled without requiring middlemen.

Table 2 Merits and demerits of various access control strategies

Access Control Model	Merits	Demerits
RBAC	- simplifies administration by assigning responsibilities to users. - Efficient for organizations with clear role structures. - Reduces administrative overhead. - Enhances security through the least privilege principle.	- Lacks flexibility in dynamic or complex environments. - Can become complex if too many roles are defined. - Not suitable for fine-grained access control needs.
ABAC	- Highly flexible and dynamic, suitable for complex policies. - granular access control is determined by many factors (environment, resource, and user). - Supports context-aware and adaptive security policies.	- Can be difficult to manage and understand complex policies. - Requires sophisticated infrastructure and more processing power. - Potentially high initial setup and maintenance costs.
MAC	- Provides a high level of safety through centralized control. - Suitable for environments requiring stringent security measures (e.g., military, government). - Prevents unauthorized information flow (strong confidentiality and integrity).	- Inflexible, making it difficult to implement in dynamic environments. - Can lead to high administrative overhead due to rigid controls. - Users have no discretion in access decisions, potentially limiting usability.
DAC	- Flexible and user-friendly, allowing resource owners to control access. - Easy to implement and manage in small and medium-sized environments. - Suitable for environments where data sharing is frequent and necessary.	- Less secure, as users might unintentionally grant excessive permissions. - Vulnerable to malware and privilege escalation attacks. - Lack of centralized control can lead to inconsistent security policies.
ReBAC	- Allows for dynamic and context-sensitive access decisions based on predefined rules. - Effective for environments requiring adaptive security measures (e.g., IP address, time of day). - Enhances security by enforcing specific conditions for access.	- Complex rule management can be difficult to scale and maintain. - Rules need to be regularly updated to remain effective, which can be resource-intensive. - Over-reliance on specific rules can lead to security gaps if not comprehensively defined.

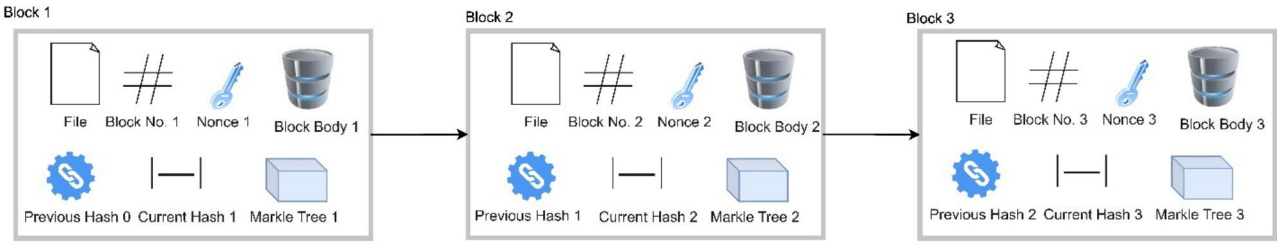

Fig. 7 Basic structure of blockchain

This automation can optimize intricate procedures, lower expenses, and mitigate the likelihood of conflicts.

The success of blockchain, especially in the commercial space, proves its importance. Currently, the blockchain market is estimated to be at $1,431 million and it is expected to grow at a CAGR of 80.2% in the global market. 54 billion by 2030, with an estimated compound annual growth rate (CAGR) of approximately 85%. 9% in the period between 2022 and 2030 [36]. Technology fuels the increase in enhancing the level of openness, safety, and productivity across various sectors. Blockchain technology is a revolutionary step in the field of business particularly in the world of transactions. The fact that this approach is decentralized, immutable, and transparent makes it a powerful medicine to the security and trust issues that are inevitable in conventional systems. The use of technology is expected to grow in various fields as technology adapts and is integrated into more areas of life, and thus the effects will be more widespread.

Research methodology

In light of this, to develop an understanding of the effectiveness and impact of the proposed blockchain-based access control in cloud environments, a systematic literature review (SLR) [37] approach is used. This methodology will closely adhere to the framework laid down by [38] to make the process of review more rigorous and exhaustive. The SLR aims at identifying, assessing, and combining prior studies that are related to the research issue under investigation. This will give a hindsight on how blockchain can be implemented in the cloud for access control.

Development of review protocol

This will involve developing a protocol for the systematic literature review to ensure that the review process is highly structured. This protocol will describe the stages of the review process and the criteria to follow when identifying and evaluating the studies.

Locating studies

Utilizing multiple electronic databases renowned for scholarly research, including but not limited to:

- IEEE Xplore (www.ieeexplore.ieee.org/Xplore/).
- SpringerLink (www.springerlink.com/).
- ACM Digital Library (www.portal.acm.org/dl.cfm).
- Elsevier ScienceDirect (www.sceincedirect.com/).
- MDPI Online (https://www.mdpi.com/journal).
- Google Scholar (http://scholar.google.com.au/).
- Emerald Insight (https://www.emerald.com/insight/).
- Wiley Online Library (https://onlinelibrary.wiley.com/).

The Boolean operators "AND" and "OR" are used to search for appropriate combinations of literature. The strings used for searching from different databases are "blockchain," "access control," and "cloud computing." The search strategy will be refined iteratively to ensure comprehensive coverage. The inclusion criteria shall cover peer-reviewed papers, book sections, or conference proceedings that have been published in English up until the present date. The study selection process is defined in Fig. 8 with all 4 states and its inclusion and exclusion criteria.

Screening and study selection

The screening process will involve distinct stages:

- Conduct a thorough examination of titles to discover relevant studies that specifically explore the use of blockchain for access control in cloud environments.
- Analyzing abstracts to determine their conformity with the research scope and objectives.
- Conducting a comprehensive analysis of publications to decide their final inclusion based on predetermined criteria.

Data extraction and synthesis

- Studies that match the specified criteria are included in a qualitative analysis procedure to collect and synthesize data systematically.
- A thematic analysis is conducted to identify emergent themes and patterns related to blockchain-based access control in cloud environments.

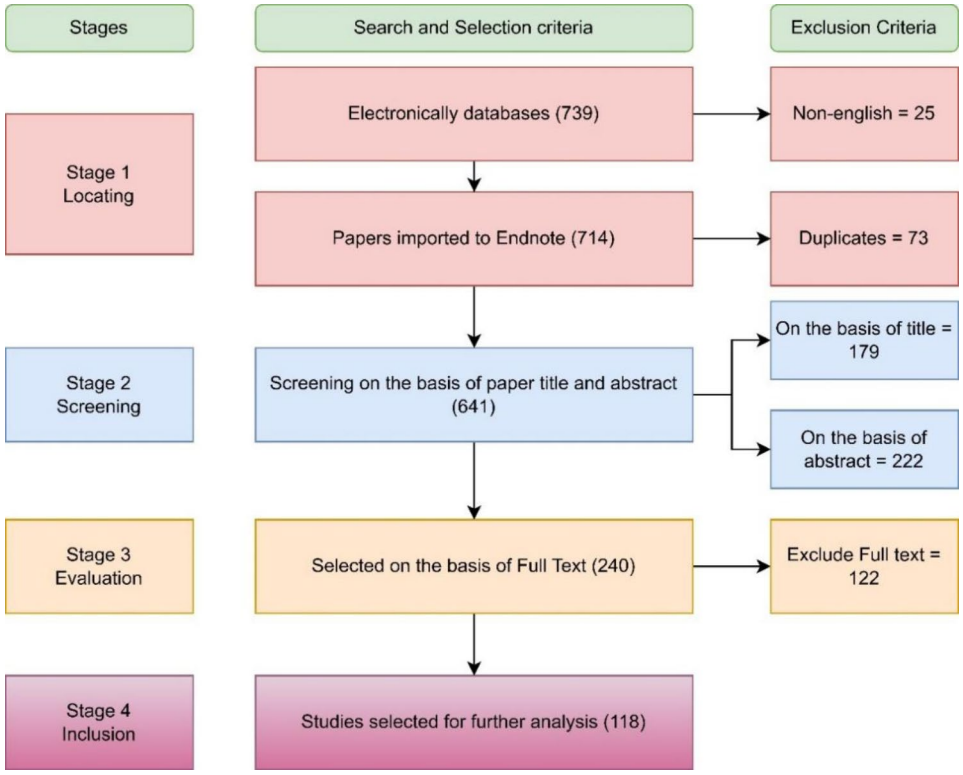

Fig. 8 Study selection process

- To guarantee the validity and dependability of the combined results, researchers will look for consensus.
- The extracted data will be organized, categorized, and synthesized to provide insights into the current state, trends, and implications of blockchain for access control in cloud environments.

Out of the 118 publications that were examined, the majority of them, which amounted to 36 papers, were obtained from IEEE databases. This demonstrates the widespread effect and contribution that IEEE has made within the realm of scientific research. Immediately following closely behind are ten papers, which constitute a sizeable portion, which originate from the Springer database. This highlights the relevance of their scholarly publications within the subject itself. The other papers, which make up the rest of the corpus, are derived from a variety of databases. This indicates that the research landscape makes use of a wide variety of sources. It is representative of the interdisciplinary nature of modern academic study. This distribution illustrates the multiple strategies that researchers adopt to obtain and integrate material from a variety of platforms. So that they can expand the discourse and progress knowledge across a variety of domains.

Over the years, the selected research articles show a significant trend in study dispersion. The year 2018 saw the publication of three publications, which is indicative of a modest beginning to the investigation of the selected subject. Scholars are increasingly interested, as evidenced by the fact that this number doubled in 2019. The number of articles published in 2020 grew dramatically, and seven research met our selection criteria. This might indicate that the area is receiving more attention and funding. The subsequent year, 2021, is indicative of a growing corpus of research and an increase in the amount of intellectual engagement. In the year 2022, the trend continued to grow significantly; we selected the highest of 43 papers, which demonstrated a significant expansion in the amount of research efforts implemented. While 2023 continued to maintain a healthy momentum with 41 publications, 2024 experienced a good start with 3 papers. Scholars highlight a progressive and dynamic landscape of scholarly investigation, marked by expansion, consolidation, and periodic changes.

Among the 118 total studies analyzed, the literature was diversified across various categories. Review articles—13 studies—provided in-depth insights into research and knowledge gaps. Most of the papers were research articles from different journals, with 63 studies focused on original empirical investigations and theoretical contributions. Forty works were published in

conference proceedings, highlighting academic and professional discussions. Though there were just two book chapters, they presumably explored distinct issues within broader academic contexts. This distribution underscores the diverse nature of scholarly contributions within the field. It ranges from critical evaluations to original research and collaborative discussions.

Blockchain-based access control

This is decentralized and tamper-resistant, improving security and transparency. This design keeps permissions in a secure, immutable blockchain ledger that requires network authorization to modify. Individual digital identities and preset smart contracts regulate access. Smart contracts define access conditions and store them on the blockchain. An access control system for a cloud environment based on blockchain technology is shown in Fig. 9.

Secure access control uses decentralized identity management and cryptographic user verification. This method promotes accountability, reduces unauthorized access, and provides a transparent audit trail for access activities. When security infrastructure needs trust, transparency, and tamper resistance, blockchain-based access control appeals. Blockchain-based access control features:

a) **Decentralization and Trust**: Decentralized authority is a major benefit of blockchain-integrated access control. Traditional models authenticate and authorize users centrally [39–41]. Centralization increases security risks since undermining the central authority could allow unwanted access and data breaches. Blockchain delegates authority to nodes, eliminating central authority. For each network applicant has a blockchain copy and consensus processes that add legitimate transactions. Decentralization makes access control more secure by reducing central authority vulnerabilities.
b) **Transparency and Accountability**: Blockchain technology makes access control transparent, improving accountability [42]. All blockchain users can see each transaction. Transparency tracks and audits changes and access attempts, creating an immutable record [43]. Traditional access control systems are opaque, making security breaches and unlawful access difficult to detect. Blockchain's clear trail deters crime and speeds up and improves incident response.
c) **Smart Contracts for Automated Authorization**: Blockchain-based smart contracts redefine access control automation. These contracts set criteria for access [44]. Smart contracts program access control, reducing manual intervention. Smart contracts can execute specified actions depending on time-based access constraints or user role changes [45]. Programmability makes cloud access control solutions more flexible and efficient. It meets changes in business needs while ensuring security and compliance.
d) Centralization, weaknesses, and lack of transparency limit traditional access control.

Traditional centralized identity management is subject to security breaches if the central authority is compromised. Limited transparency and accountability in centralized access logs may compromise data integrity [46]. Blockchain-based access control systems tackle these issues through decentralization and tamper-resistant ledgers. Decentralized identity management and access logs improve blockchain security by eliminating a single point of failure. By archiving access control decisions, the blockchain ledger's openness and immutability address accountability and data integrity issues. Blockchain-based

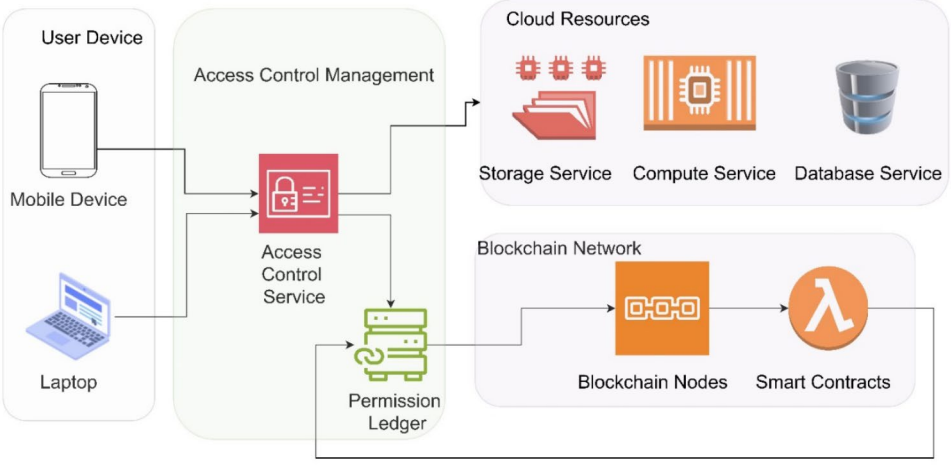

Fig. 9 The block diagram of blockchain-based access control

access control is safer and more automatic due to cryptographic verification and smart contracts. Table 3 shows how blockchain-based access control overcomes system issues in traditional access control systems.

Many researchers and practitioners have investigated the incorporation of blockchain technology into access control systems for cloud computing. Prior research has focused on using blockchain technology to automate access control decisions, ensure secure and auditable access records, and facilitate the execution of smart contracts. These initiatives aim to enhance the security, transparency, and efficiency of cloud access control while also addressing difficulties commonly found in traditional models. Efficient blockchain-powered access control solutions for cloud computing require a comprehensive understanding and enhancement of previous research efforts. The mainstream of blockchain-based access control is further divided into 12 sub-streams, as shown in Table 4, and then, based on this, the literature review is carried out.

Enhancing data integrity and immutability

Fixed-size hash values are produced from variable-size input data by cryptographic hash algorithms. These features guarantee the accuracy of the information by detecting any attempt to change or modify the data. For example, Bitcoin's blockchain uses SHA-256, which produces a 256-bit hash value. In blockchain technology, various hash functions are used. The most extensively utilized hash functions are listed in Table 5. These functions are essential for ensuring data consistency among nodes in a dispersed network. Every node retains a copy of the ledger and consensus mechanisms. It assures that all nodes achieve a consensus on the validity of transactions, thereby maintaining data consistency. Moreover, due to the nature of the blockchain, data storage is also protected from alteration of information stored within it. After a record is made in the ledger, it cannot be altered or deleted without consensus from the majority, which makes it safe from manipulation. The decentralized and consensus-driven architecture of this system also guarantees that any form of illegality in data alteration or forgery is tackled hence improving the credibility and reliability of access control systems.

Sandeep Kumar and Suresh used SeFra, a temporal blockchain technique, in the Secure Health Framework to improve context-based access restriction, secrecy, and integrity verification. SeFra uses the Context-based Merkle Tree (CBMT), temporal characteristics, HL7 protocols, and IPFS to secure Personalised Micro Ledger (PML) and assure interoperability and scalability [65]. SeFra records temporal health records and shares them using context-aware smart contract rules to resolve data silos and secure healthcare transactions. Despite blockchain's promise to improve EHR interoperability and privacy, scalability, usability, and accessibility remain, as does the need for secure access control. It also stores medical records off-chain and provides timely access during emergencies.

Kumar et al. [66] highlighted weaknesses in prior validation systems and noted that security problems still exist even after post-2017 fixes. They found insider

Table 3 Comparative study of traditional and blockchain-based access control system

Feature	Traditional Access Control System	Blockchain-Based Access Control System
Identity Management	Centralized identity management (e.g., single sign-on solutions)	Decentralized identity management (individual cryptographic keys)
Ledger for Access Logs	Centralized logs with potential vulnerabilities and single points of failure	Decentralized, tamper-resistant blockchain ledger for transparent and immutable access logs
Smart Contracts for Access Rules	Limited automation, often manual rule implementation	Self-executing smart contracts encode access rules and automate enforcement
Cryptographic Verification	Relies on traditional authentication methods (e.g., passwords)	Utilizes public-private key cryptography for secure user identification
Transparency and Audit Trail	Centralized logs may lack transparency and accountability	Transparent and auditable history of access control decisions on the blockchain
Consensus Mechanism	Centralized decision-making authority (e.g., role-based approval)	Decentralized consensus mechanism for access control decisions
Granular Access Control	Limited granularity and flexibility in defining access conditions	Fine-grained control with dynamic conditions based on smart contracts
Interoperability with Cloud Services	Integration challenges and dependencies with existing cloud services	Designed for seamless integration with existing cloud infrastructure
Dynamic Access Management	Limited adaptability to changing circumstances or user behaviour	Dynamic management based on evolving conditions and user behaviour
Privacy Protection	Limited control over personal data handling and potential privacy issues	Improved privacy with cryptographic techniques (e.g., zero-knowledge proofs)
Tokenization of Access Rights	Traditional access tokens with limited flexibility	Tokenization of access rights on the blockchain for secure representation and transfer of permissions

Table 4 Blockchain based access control features and associated goals for advanced system capabilities

Features	Associated Goals
1. Enhancing Data Integrity and Immutability	1. Implementing Cryptographic Hash Functions 2. Enforcing Data Consistency Across Nodes 3. Providing Tamper-Proof Data Storage 4. Preventing Data Manipulation and Forgery
2. Facilitating Decentralized Governance and Consensus	1. Implementing Decentralized Decision-Making Processes 2. Enabling Distributed Consensus Mechanisms 3. Supporting Stakeholder Participation and Voting 4. Ensuring Transparent Governance Structures
3. Ensuring High Availability and Fault Tolerance	1 Implementing Redundant Data Replication Strategies 2. Enabling Automated Failover Mechanisms 3 Supporting Disaster Recovery and Backup Solutions 4 Ensuring Continuous Access to Resources
4. Enabling Interoperability with Existing Systems	1. Integrating with Legacy Access Control Mechanisms 2. Supporting Standardized Protocols and APIS 3. Enabling Seamless Data Exchange Between: Platforms 4. Facilitating Integration with Third-Party Services
5. Enhancing Scalability and Performance	1. Implementing Sharding and Horizontal Scaling Techniques 2. Optimizing Transaction Throughput and Processing Speed 3. Supporting Elastic Resource Provisioning and Auto-Scaling 4. Ensuring Efficient Resource Utilization and Load Balancing
6. Empowering User-Centric Access Control	1. Enabling Self-Sovereign Identity Solutions 2. Providing User-Managed Access Policies 3. Supporting Granular Permission Management 4. Facilitating Consent-Based Data Sharing
7. Promoting Transparency and Auditability	1. Recording Access Control Events on a Public ledger 2. Providing Immutable Audit Trails for Compliance 3. Enabling Real-Time Monitoring and Reporting 4. Facilitating Forensic Analysis and Incident Response
8. Enhancing Security with Multi- Factor Authentication	1. Implementing Biometric Authentication Methods 2. Enforcing Hardware-Based Security Measures 3. Supporting Time-Based One-Time Passwor's (TOTP) 4. Integrating with Eardware Security Modules (HSMs)
9. Facilitating Regulatory Compliance and Reporting	1. Ensuring Compliance with Data Protection Regulations (e.g., GDPR HIPAA) 2. Providing Audit Reports for Regalatory Authorities. 3. Enabling Secure Data Retention and Archiving. 4. Supporting Regulatory Standards for Access Control
10. Empowering Edge Computing and loT Devices	1. Integrating Access Control Mechanisms into Edge Noces 2. Enabling Secure Communication Channels for loT Devices 3. Lightweight Access Control Protocels for Edge 4. Facilitating Authentication and Authorization at the Edge
11. Enabling Transparent Supply Chain Management	1. Recording Supply Chain Transactions on a Blockchain 2. Providing End-to-End Traceability of Goods and Materials 3. Ensuring Compliance with Supply Chain Regulations 4. Facilitating Audits and Inspections Across the Supply Chair
12. Supporting Immutable Digital Identities	1. Storing Digital Identity Attributes on a Blockchain 2. Enabling Portable and Interoperable Identity Crecentials 3. Ensuring Trustworthy Identity Verification Processes 4. Facilitating Secure Authentication and Authorization Processes

attacks and password prediction were among the weaknesses that newer approaches unintentionally added. They developed a lightweight computational validation system, evaluated it using the AVISPA tool, and showed that it was resistant to different kinds of attacks. The suggested approach has higher storage costs even if it demonstrates efficiency in computational overhead.

To enhance security, particularly for sensitive data like institutional databases, Jia et al. [67] investigate how blockchain technology might be integrated into cloud storage and provide search access. They suggest a dynamic, verifiable ciphertext retrieval method that uses Ethereum's features for controlled access. It also makes sure the results are right even if the server is malicious. The innovative data update verification system uses aggregated message authentication code technology for forward and backward privacy. Experimental tests show

Table 5 Different hash functions implemented on different blockchain platforms

Hash Function	Platform	Algorithm	Output Length	Description
SHA-256 [47]	Bitcoin, Ethereum	SHA-256	256 bits	Secure Hash Algorithm 256-bit is widely used in blockchain for hashing blocks, transactions, and cryptographic operations.
SHA-3 [48]	Ethereum	Keccak-256	256 bits	SHA-3 is based on the Keccak sponge construction and is used in Ethereum for hashing smart contracts and data.
Blake2b [49]	Cardano, Tezos	Blake2b	Variable	Blake2b stands for the improved cryptographic hash function as compared to the Blake and it is more efficient in speed. It is employed in Cardano and Tezos blockchains for different purposes.
Scrypt [50]	Litecoin, Dogecoin	Scrypt	Variable	Scrypt is a password-based key derivation function that is used in Litecoin and Dogecoin for proof-of-work mining and key generation.
RIPEMD-160 [51]	Bitcoin	RIPEMD-160	160 bits	RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) is used in Bitcoin to generate public addresses from public keys.
SHA-512 [52]	Hyperledger Fabric	SHA-512	512 bits	SHA-512 is a variant of SHA-2 and is used in Hyperledger Fabric for hashing blocks, transactions, and cryptographic operations.
BLAKE2s [53]	Zcash	BLAKE2s	Variable	BLAKE2s is a variant of BLAKE2 optimized for speed and used in Zcash for hashing blocks and transactions.
X11 [54]	Dash	Multiple	Variable	X11 is a chained hashing algorithm that combines multiple hashing functions (Luffa, Blake, Shavite, JH, Keccak, Cubehash, Groestl, SIMD, Skein) and is used in Dash for mining.
Ethash [55]	Ethereum	Ethash	Variable	Ethash is a memory-hard proof-of-work algorithm used in Ethereum to mine new blocks and validate transactions.
SHA-1 [56]	Bitcoin, Ethereum	SHA-1	160 bits	Secure Hash Algorithm 1 (SHA-1) is an older hash function used in some blockchain applications, although it is less secure than SHA-256 and SHA-3.
Keccak [57]	Ethereum	Keccak	Variable	Keccak is the cryptographic sponge function upon which SHA-3 is based. It is used in some Ethereum-based applications for hashing and encryption.
Argon2 [58]	Ethereum	Argon2	Variable	Argon2 is a memory-hard hashing function designed for password hashing and key derivation. It is used in Ethereum for certain cryptographic operations.
Groestl [59]	Groestlcoin	Groestl	Variable	One of the hashing algorithms used for proof-of-work mining and transaction verification on the Groestlcoin blockchain is called Groestl.
Whirlpool [60]	Monero	Whirlpool	Variable	Whirlpool is a cryptographic hash function used in some privacy-focused blockchains like Monero to hash transactions and maintain anonymity.
Skein [61]	Skeincoin	Skein	Variable	Skein is a cryptographic hash function used in Skeincoin for proof-of-work mining and block validation.
Cryptonight [62]	Monero	Cryptonight	Variable	Cryptonight is a memory-bound hashing algorithm used in Monero and other cryptocurrencies to mine new blocks and validate transactions.
NeoScrypt [63]	Feathercoin	NeoScrypt	Variable	NeoScrypt is a hashing algorithm used in Feathercoin and other cryptocurrencies for proof-of-work mining. It is known for its memory hardness and resistance to ASIC mining.
Lyra2REv2 [64]	Vertcoin	Lyra2REv2	Variable	Lyra2REv2 is a hashing algorithm used in Vertcoin for proof-of-work mining, designed to resist both ASIC and GPU mining, promoting decentralization.

that the method works well for creating, retrieving, and checking indexes.

Zuo et al. [68] introduce CP-ABE and multi-chain-structured blockchain-based data exchange to provide ownership, confidentiality, and fine-grained access control. Real-time attribute maintenance is made possible by attribute-token-based revocation in smart contracts, which also enable on-chain and off-chain interactions. Fabric experiments demonstrate that this decentralized approach offers a secure platform for data sharing while resolving centralized design issues.

Algarni et al. [69] propose a Multi-agent system for decentralized, lightweight IoT access control protection while admitting the drawbacks of both centralized and decentralized approaches. With Blockchain Managers (BCMs) their approach addresses IoT system scalability and performance. A RaspberryPI IoT device and private blockchain platform were used to test the framework in real-world circumstances, according to the research.

Boumezbeur et al. [70] use the Ethereum blockchain and cloud technology to build a EHR access control mechanism for privacy based on blockchain. They propose using Ethereum smart contracts to share EHRs with granular user access controls. Data confidentiality and privacy are protected via symmetric and asymmetric encryption. Performance on Ethereum verifies the proposal's capacity to meet security requirements.

Chen et al. [71] propose a medical data information system based on blockchain to protect the gathering, archiving, and distribution of surgical health records (SHR) and Electronic Medical Records (EMR). For effective and trustworthy SHR data collection during surgery, they created an IoTs-based data collecting system. Using blockchain technology and a proxy re-encryption

algorithm, the system guarantees protection of data against forgeries and tampering during transmission and storage. Built on Hyperledger Fabric, the system passes performance, overhead, and safety assessments to fulfil the specifications for real-world medical applications, including data mining and remote diagnosis.

Yang et al. [72] present an edge secure data access control method based on blockchain for smart grid systems to protect IoT device data. They use threshold secret sharing and ciphertext policy attribute-based encryption (CP-ABE) to effectively and safely manage data access. Computing workloads are outsourced to consortium blockchain edge nodes for flexible data exchange using on-chain/off-chain techniques. Security and performance evaluation, including Raspberry Pi on Hyperledger Fabric simulation, establish the scheme's security and efficiency for lightweight IoT devices in smart grid contexts.

Liu et al. use [73] Casbin, chaotic encryption, LSB technology, and ABAC to secure IoT data privacy with an access control paradigm based on blockchain. Hyperledger Fabric stores dynamic access control strategies in blockchain blocks, enabling updates and single-point resiliency. The framework proves fine-grained access control amongst alliance nodes through experiments and comparisons.

Fan et al. [74] present TraceChain, a system that utilizes the E-CP-ABE and blockchain to ensure the confidentiality and traceability of data in cloud environments. Data ownership, data utilization, cloud, blockchain, and a transaction database are all involved in the system's interactions. TraceChain provides efficient tracking and fine-grained access control while protecting data with encryption and parameter sharing on a private blockchain. The proposed system is efficient and practicable, according to experiments.

Gowda et al. [75] propose BSKM-FC, a decentralized key management system based on blockchain for fog computing environments. BSKM-FC generates and shares private and public keys using a one-way hash chain with ECC. Fog servers generate session keys and store them in the blockchain. Security and overhead assessments show that Truffle Blockchain improves performance and security over conventional alternatives.

Na and park [76] address blockchain oracle and data privacy issues related to Dashcam video data dependability. Vehicles in V2V networks can group to pick transaction clients for dependable data storage and access management. This system design uses Dashcam clients to communicate with Networkhdfs and Networkfabric and decentralized oracles to verify blockchain data. Multi-signature compression, consensus techniques, lightweight blockchain, and RSU-based vehicle grouping will be studied to improve system performance and dependability.

Praveena Anjelin and Ganesh Kumar [77] explore centralized versus decentralized cloud storage architectures, stressing blockchain technology's security benefits. Decentralized storage uses blockchain, encryption, and peer-to-peer networks to protect files. An adaptive encryption method to enhance access control and distributed security is presented in this work.

Huang et al. [78] suggest BCES, an eHealth system built on blockchain, to solve the privacy and security problems in cloud-based EHRs. BCES records legal data requests and outsourcing modifications in the blockchain to protect EHR integrity and traceability. Finer access control is possible with attributes-based proxy re-encryption, and blockchain's traceability holds entities liable for illicit manipulations. Security and performance testing prove the scheme's efficacy.

To ensure the security of massive volumes of data kept in the cloud, Li [79] proposes a verifiable user data access control policy based on blockchain. This is particularly for emphasis on the interchange of medical data. The technology uses blockchain to detect and prevent questionable access, assuring data security and privacy. Securing such networks requires specialized node identification, dispersal, and access procedures, notwithstanding their complexity and cost. The suggested system is tested for resilience against hostile assaults like Eclipse, demonstrating its ability to secure and protect important application data.

Deng et al. [80] propose a blockchain-based cloud server layer architecture for Wireless Body Area Networks (WBANs), with each hub node carrying a private blockchain for sensor and patient registration data. To simplify the system, healthcare providers store physiological data. Encryption and CP-ABE are used to establish data security and access control. The architecture addresses traditional centralized architectures and network security risks like DoS and DDoS assaults to improve system stability and patient data privacy. Future research will examine practical ways to increase patient data privacy and security.

Prasad et al. [81] describe a collaborative medical image analysis system model for diabetic retinopathy diagnosis that addresses bandwidth and security issues. Blockchain is used for model storage and aggregation during data cleaning and lesion classification. Access control systems RAC and BAC provide fine-grained control and lightweight authentication. Classification accuracy and data security improved to 90.2% in experiments.

Hoang et al. [82] present a Data-sharing network for decentralized storage systems powered by blockchain that protects data security, user privacy, and availability. The platform protects user privacy and data by using blockchain technology to store secret access control lists that are publicly verifiable. The platform implements RPE

and ring signatures to test data privacy and access control. Rather than using a cloud-based approach, Zhuo et al. [83] suggested a distributed access control system based on blockchain for locally stored industrial data.

Spoorti et al. [84] proposed blockchain-based access control to address cloud computing privacy and data security problems. They secured key pairs and IP addresses on the Ethereum blockchain to avoid spying. They tested the system's scalability and performance on Ethereum using OpenStack cloud for resource provisioning, revealing its secure cloud resource access capabilities. This storage mechanism is vulnerable to several security issues, however. Blockchain technology is a sophisticated method that distributes data storage such that once it is saved, it cannot be changed. As a result, they suggest a decentralized blockchain architecture for the cloud storage platform. To provide a more secure environment, the suggested design has integrity-checking and access control features. Additionally, it offers four main services that provide security elements in a cloud storage system:

(i) Data owners save user data Meta details in the blockchain structure and set access rules to maintain the authorization feature;
(ii) The cloud storage system stores the original data and uses the optimization algorithm to reduce the transaction processing time;
(iii) Data owners maintain the data integrity using the Merkle root concept.
(iv) A registration process is designed to register data owners and users using a key generation technique to provide an authentication feature. The experimental findings, analysis, and performance assessment show that our suggested design offers a workable and dependable cloud environment.

Kumar et al. [85] recommend using blockchain with cloud computing to improve cloud security. Blockchain technology, along with cloud security, provides a decentralized and digitized method of recording transactions. This is made possible through the use of sophisticated computing techniques and cryptographic locking systems. Blockchain ensures the preservation of confidentiality, integrity, anonymity, availability, and privacy. This proactive strategy proposes utilizing blockchain technology to enhance cloud security, mitigate attacks, and assess risks.

Wang et al. [86] discuss potential data availability issues and Attribute-Based Encryption (ABE) restrictions in traditional cloud storage based on trusted Private Key Generators. Instead of a trusted PKG, they propose merging IPFS, Ethereum blockchain, and ABE. Decentralizing secret keys allows data owners to share them, improving flexibility and reducing key misuse. Access policies enable fine-grained access control. Smart contracts on Ethereum fix cloud storage issues, ensuring accuracy.

Gao et al. [87] introduced a trustworthy attribute-based searchable encryption (ABSE) system. Blockchain technology was used to create a system of rewards and penalties specifically for ABSE. It also makes it easier to search using many keywords. The Data Owner (DO) uploads more data to the blockchain and provides ciphertext indices to a Searchable Encryption Service Provider (SESP). The SESP utilizes a distinctive blockchain system that rewards and penalizes participants to ensure the production of accurate search results within a predetermined block height. Economic incentives, such as reduced penalty costs, promote honesty. The blockchain serves as a reliable and fair system by penalizing dishonest participants and establishing trust.

Zhang et al. [88] discuss MCC authentication and access control. The two major privacy issues that are highlighted in MCC include ownership rights and user identities. The proposed system that uses blockchain technology for authentication can be audited, anonymous, and has a hierarchical architecture. Their concern is on addressing the issues of how to deal with MCC in the context of authentication and access control. MCC users' access permissions and identities are the main concerns of privacy. Proposed solutions include the use of hierarchical access control based on blockchain technology and auditable authentication. The technique conceals rights with Pedersen's commitment, and the dynamic pseudonyms to anonymise users. The above-mentioned method satisfies the security requirements of MCC after the security analysis is carried out. The experimental results reveal that the suggested strategy takes less communication cost than the existing technique when adopted in Hyperledger Fabric.

The study discussed in the present paper demonstrates how blockchain has already emerged as a critical enabler for privacy, security, and access control in cloud computing, IoT, and health care as well as data sharing. Scholars present innovative ideas and concepts by leveraging blockchain's distributed nature, self-executing smart contracts, cryptography, and consensus algorithms to address the problems of data authenticity, system capacity, compatibility, and secure access control. These solutions leverage blockchain, cloud, IoT and edge computing to build robust, decentralized structures that secure data, privacy and access and minimize threats posed by centralised storage and access control solutions. This paper's experimental findings indicate that using blockchain for access control is possible, effective, and efficient, which suggests that this technology could revolutionize data storage and ensure the security of various forms of data.

In this paper, the issues of scalability, practicality, efficiency and implementation challenges that are related to the correct implementation of the advantages of blockchain technology when used in modern computer environments to improve access control and data security are identified and analyzed.

Facilitating decentralized governance and consensus

Blockchain technology disrupts the decision-making procedures since it does not require the involvement of a central authority. Likewise, PoW and PoS enable nodes to sign for transactions and arrive at consensus without relying on third parties. By employing auditable voting systems, decentralization empowers stakeholders to make transparent decisions, thereby increasing the level of democracy. Furthermore, the public ledger of blockchain documents every transaction and governance decision, guaranteeing openness and accountability in governance systems. As it is a fundamental principle of blockchain technology.

Ravikumar Ch et al. [89] describe a blockchain-assisted cloud-stored EHR system that safeguards data, user privacy, data quality, and fine-grained access control. The proposed solution uses a consortium blockchain to handle user groups inside healthcare organizations. For data integrity and privacy, search terms and updated hash values for medical records are kept on the consortium blockchain. The blockchain's search phrases split patient EHRs, giving specialized individuals access to records. Users can access encrypted cloud-based EHRs using an attribute-based contract key for fine-grained medical record access. EHRs could be stored via IPFS, a decentralized and distributed storage system. Accessing these records via the blockchain would eliminate the need to trust third-party cloud providers.

Le et al. [90] offer A blockchain-based access control system called CapChain for sharing and delegation. Blockchain architecture makes the framework reliable. CapChain also protects user privacy by hiding access delegation data. The study describes CapChain as a secure and private access control solution for IoT applications.

Wang et al. [91] offer a safe cloud-based EHR solution to overcome EHR security concerns. The main innovation is the C-AB/IB-ES scheme, which combines encryption and signature functions. This method simplifies system management and eliminates the need for several cryptographic systems for security. Blockchain technology ensures medical data integrity and traceability, improving EHR security. Subsequent investigations will include implementing smart contracts on the suggested framework and developing an automated insurance claim agreement on the Ethereum network.

To increase cloud security, Kumar et al. [85] advise combining blockchain technology with cloud computing. Blockchain technology offers a digital and decentralized way to record transactions, especially when combined with cloud security. This is made possible through the use of sophisticated computing techniques and cryptographic locking systems. Blockchain ensures the preservation of confidentiality, integrity, anonymity, availability, and privacy. This proactive approach suggests using blockchain technology to improve cloud security, lessen threats, and evaluate hazards.

To reduce security risks, Yan et al. [92] suggest a decentralized cloud storage architecture built on blockchain that includes integrity checking and access control. The major services were registration, access controls, storage optimization, and data integrity maintenance. For security and integrity, the proposed architecture makes use of distributed key generation, Merkle root, and ciphertext attribute-based encryption. Empirical findings demonstrate the viability and dependability of the proposed system.

Tan et al. [93] developed a framework based on blockchain for generic Green IoT (GIoT) access control to simplify heterogeneous Green Smart Device user administration. DIDs give users and GSDs visible identities for authentication. This framework uses blockchain's decentralization and tamper-resistance to establish a unified GSD access control system for registration, giving, and revoking permissions. The framework can offer decentralized, lightweight, and fine-grained access control for GSDs, according to testing conducted on Raspberry Pi and FISCO-BCOS. It also improves immutability, scalability, accessibility, and the reliability of data.

Truong et al. [94] introduced CapBlock, a blockchain with DCapBAC and smart contracts for access control. For policy and capability management, CapBlock leverages Hyperledger Fabric and two smart contracts; its throughput and latency are similar to those of non-blockchain DCapBAC. Cryptographic key schemes such as CP-ABE and the production of authentication credentials are proposed for a decentralized IoTs architecture that enhances data security.

Deebak et al. [95] developed RB-LDA for 5G networks to solve IoT device security and privacy. For enhanced auditing, RB-LDA authenticates device access, prevents key exposure, and continually analyzes IoT device operations. Experimental results show that RB-LDA improves data privacy against trusted third parties, improving cloud storage data integrity. The study also presented a lightweight identity-based cloud auditing strategy with batch auditing to reduce key exposure damage and aims to use smart contracts for quicker transaction rates.

Marwan et al. [96] presented an IoT- and cloud-specific distributed security approach to secure patient medical records. They used OM-AM for security needs analysis and a blockchain architecture with ABAC for

decentralized access control. They strengthened cloud-enabled IoT security for smart healthcare by using XACML to create strong policies.

Nguyen et al. [97] presented a cooperative healthcare architecture employing edge-cloud computing and Ethereum blockchain for data dumping and sharing. A privacy-aware data offloading strategy for IoT health data with blockchain for secure user data exchange ensured data privacy and access management via smart contracts. In comparison to earlier systems, testing revealed improved QoS, data privacy and security, and low smart contract costs. It shows that the proposed approach was feasible and effective for healthcare applications.

Tariq et al. [98] suggested a safe way to share healthcare data that would use blockchain and the InterPlanetary File System (IPFS) to deal with privacy and security issues. Users had varying access rights with fine-grained access control utilizing smart contracts on an Ethereum private blockchain. AES-256 and Diffie-Hellman key exchange encrypted data, while IPFS prevented single points of failure and ensured data availability. Establishing data-sharing access levels improved the system's efficiency. However, user anonymity and research organization data delivery might be added.

Malamas et al. [99] presented a hierarchical multi-blockchain architecture to manage granular health data access and meet the complicated security and privacy concerns of networked healthcare stakeholders. In this architecture, separately managed trust authorities can cooperate at the top layer while each domain enforces fine-grained access control regulations with attribute-based encryption at the bottom layer. Ciphertext-policy attribute-based encryption (CP-ABE) speeds up credential revocation and decentralized policy enforcement with smart contracts. The system offers safe, interoperable data access, adaptive capacity, distributed trust management, and dependable forensics. However, finding improved consensus methods for security and scalability, scaling up implementations, and streamlining intra-blockchain communication and consolidation are areas for advancement.

The literature review shows how blockchain technology's decentralised governance models affect decision-making. Through verifiable voting, consensus algorithms like PoW and PoS enable decentralised agreement among nodes, promoting transparent decision-making and democratic government. The public ledger's transparency and accountability enable open governance systems, matching with blockchain technology's core ideals. The presented frameworks and solutions show that blockchain can improve data security, privacy, integrity, and fine-grained access control in healthcare, IoT, and cloud computing. Blockchain technology enables more inclusive, secure, and transparent decision-making.

Ensuring high availability and fault tolerance

Blockchain networks replicate data over numerous nodes to improve fault tolerance and availability. Redundancy reduces data loss and downtime, ensuring resource availability. Blockchain platforms also have automated failover capabilities that quickly detect and transfer transactions and data to operational nodes to minimize service disruptions and maintain platform availability. Through its distributed architecture, blockchain provides disaster recovery and backup by decentralizing data storage and duplicating data across nodes in different contexts. Due to blockchain technology's fault tolerance and automated failover, access control systems can remain available during network outages or node failures.

Wang et al. [100] put out a blockchain-based solution for secure cloud storage access control. To increase security, Ethereum's smart contract technology has been included in the ciphertext-policy attribute-based encryption method. A central authority no longer controls the distribution key, rendering the scheme decentralized. The system uses distributed access control, where the data owner and user nodes communicate. Experimental results show low file access costs. The solution uses a semi-honest cloud storage infrastructure; thus, more research is needed. Data integrity research is lacking, preventing data owners from tampering with uploaded documents. Decentralized storage platforms like InterPlanetary File System (IPFS) and Storj may replace traditional cloud storage platforms in the future. It indicates an awareness of evolving technologies and potential framework improvements.

Singhal et al. [101] discuss the inefficiencies and security risks of traditional document verification and centralized digital locker systems. They offer an Ethereum-based decentralized solution for safe personal document storage. This solution simplifies verification, secrecy, access control, data privacy, authenticity, and document integrity.

Sharma et al. [102] describe a blockchain-based cloud storage architecture for privacy and distributed access control. They generate keys using ciphertext attribute-based encryption, improving distributed system security. Access control and Merkle roots support data privacy and integrity in the blockchain framework. Honeybee optimization speeds transactions. The next steps include user revocation for security and dynamic access management.

Tharani et al. [103] proposed a blockchain-based IoT database management solution to secure and monitor data access. Smart contracts manage database operations, whereas distributed ledger hash pointers track data off-chain. Data identification and client targeting are improved, and new capabilities are added to IoT apps using this method.

Haritha and Anitha [104] emphasize healthcare access control and provide a secure framework using LBAC and blockchain-based smart contracts. The method improves data security while providing confidential user access. In a decentralized system, smart contracts ensure transaction integrity, and LBAC provides layered protection. Compared to existing solutions, the suggested model better protects privacy, openness, and data integrity. Future research is needed to address shortcomings and improve the framework's scalability and real-world use.

Xiao et al. [105] solve traditional data-sharing system issues by focusing on decentralized user revocation. They offer MAFR-KP-ABE for decentralized authorization and flexible revocation. Through comparison with applicable schemes, security and efficiency are verified. Finally, MAFR-KP-ABE and blockchain are used to create a fine-grained access control system with security analysis and implementation to demonstrate efficiency and security.

Sharma and Sharma [106] cover access control, security, and privacy in decentralized IoT systems. Their cutting-edge methodology includes the cross-agency architecture and the Bitcoin blockchain. To handle secure, decentralized, and lightweight access delivery in the IoTs networks, Bitcoin Administrator is being developed. It enables encrypted communications between regional devices.

Liu et al. [107] discuss zero-trust cross-domain data sharing issues in the cloud-edge-end architecture. They propose solutions for security, fairness, scalability, and efficiency. This includes creating a new plaintext checkable encryption technique for IoT devices, a sharding blockchain-based multi-domain architecture, and partial trust and zero-trust data exchange schemes.

Rohini et al. [108] suggest using blockchain in IIoT to ensure immutable and indisputable services. They use a hierarchical blockchain system with older blocks in the mist and fresh blocks in overlay networks to scale. The suggested system enables graded blockchain with blockchain, IIoT, and cloud overlay networks. A versatile cooperative ownership and access management framework for lightweight IoT devices is also presented. Experimental results show that hierarchical blockchain storage in an IIoT application is efficient.

Zhang et al. [109] propose a blockchain-based hierarchical data sharing framework (BHDSF) as a solution to issues with the existing HIoT systems. With effective key distribution and access management, BHDSF secures PHR sharing and prevents privacy leakage and integrity violation. Untrusted cloud and malevolent auditor situations are considered for trustworthy PHR integrity auditing. The methodology provides aggregative authentication for source record trustworthiness, which conventional methods lack. Comprehensive empirical tests on real-world data prove it.

Sravanthi and Chandrasekhar [110] introduce the Multi-User Groupwise Integrity Ciphertext-Policy Attribute-Based Encryption (GI-CPABE) architecture for cloud blockchain EHR security. GI-CPABE provides role-specific and reliable access control via the use of heterogeneous cloud-compatible Improved Ciphertext-Policy Attribute-Based Encryption (ICP-ABE). Integrity is increased by the role-based access system, which effectively grants user access rights based on the characteristics of multi-user groups. A real-time cloud server was used to test time efficiency, storage utilization, data integrity, and safe access. Comparative analysis showed strong role-based access control.

The literature analysis shows how blockchain networks' fault tolerance and redundancy features improve access control system availability during network outages or node failures. Blockchain technologies reduce downtime by replicating data across several nodes and automating failover. Blockchain networks' decentralized architecture distributes data storage and duplicates data across nodes, making disaster recovery and backup easier. Even during network infrastructure failures, these characteristics ensure access control system availability and dependability. Proposed frameworks and protocols demonstrate that blockchain technology might revolutionize access control by delivering secure, decentralized, fault-tolerant solutions that prioritize system availability and resilience.

Enabling interoperability with existing systems

Companies can enhance their access control expenditures on infrastructure with blockchain-based access control solutions that integrate seamlessly with legacy systems. Blockchain platforms improve interoperability and versatility by using known protocols and APIs to work with a variety of cloud-based services, applications, and identity management systems. Blockchain's decentralization allows secure and transparent data interchange between platforms and ecosystems, fostering interoperability and data sharing. Blockchain-based access control systems can also integrate with third-party services and platforms like identity verification providers and compliance solutions. It improves their functionality and enables continual improvement and extension.

Showkat and Qureshi [111] address big data analytics for strategic investments and data storage security issues. They note that private companies hold most cloud servers, affecting data privacy. The author suggests a blockchain-powered decentralized system for data trust and user control to overcome these concerns. Blockchain improves data analysis and ensures correct outcomes in essential applications by providing security, privacy, access control, and data veracity.

Sarfaraz et al. [112] offer a blockchain-based system using Attribute-Based Access Control (ABAC) to protect

data in Supply Chain Management (SCM). The framework allows for flexible and detailed access control. The author proposes implementing a hierarchical network structure consisting of a worldwide ledger for recording transactions and several localized ledgers for managing access policies and commercial contracts. This approach aims to resolve the problem of scalability. To evaluate the ability to handle increasing workloads and data processing speed, the author intends to incorporate local ledgers. To enhance data processing efficiency, it is recommended that high-performance hash algorithms be utilized to optimize the current technique.

Alamri et al. [113] conducted a thorough literature review of blockchain-based IAM solutions in HIoT applications. Twenty-four research examined BC-based IAM system security, architecture, and technologies in HIoT (Health IoT). The review found that Blockchain-based IAM in HIoT lacked security frameworks, risk assessments, and evaluation criteria. BC solution security, functionality, and evaluation of BC-based IAM systems need further study.

Kawalkar and Bhoyar [114] discuss cloud security problems as cyberattacks rise and cloud infrastructure becomes more prevalent. Vulnerabilities and rigid policies plague traditional security architectures. Zero Trust Network Access, AI-Driven Security Policy Management, Federated Learning, and Blockchain are used to create a novel security framework to address these issues. Federated Learning decentralizes machine learning, Blockchain verifies transactions, AI algorithms automate security policies, and Zero Trust principles restrict access. Security metrics have improved significantly, signalling a new era of resilient cloud security systems.

Omercen et al. [115] examined the integration of blockchain and AI technology in healthcare systems, with a particular emphasis on medical imaging, electronic health data exchange, and diagnostics. The latest technical standards for the healthcare ecosystem are examined in this survey to improve data management and access control and solve security concerns.

Jayasudha and Vijaylakshmi [116] present a Safe EHR sharing using a blockchain-based Diagonal Digital Signature Algorithm (DDSA) and Merkle Patricia Hash Trie (MPHT) framework. This tackles cloud-based healthcare data privacy and network security problems. The framework allows patients and surgeons to securely share medical records while maintaining flexibility and accessibility. Practical results show enhanced access control, network latency, and data privacy compared to existing approaches. It provides a secure data interaction solution for cloud-based healthcare contexts.

Zukarnain et al. [117] highlight the necessity of implementing medical record storage and retrieval systems that are both secure and decentralized in considering recent developments in AI, blockchain technology, cloud computing, and big data. They propose a Medi-block record, a consolidated patient medical record solution for secure sharing and retrieval across healthcare providers. To protect Medi-block records, the study examines blockchain technology, access control, and privacy-preserving measures. It highlights outstanding difficulties and challenges and emphasizes the potential of medi-block records as a centralized system for safe medical data sharing in healthcare.

Chougule et al. [118] emphasize data exchange and security in IoT-cloud contexts. Secure data exchange using Proxy re-encryption and identity-based encryption is proposed. To overcome IoT device restrictions, an edge device proxy servers sophisticated calculation. By caching data, information-centric networking improves service quality and capacity. Blockchain allows decentralized data exchange, efficiency, and fine-grained access control, with security studies showing its privacy and dependability possibilities.

Singh and Singh [119] discuss decentralized blockchain's data security potential in cloud computing and IoT. Access control, user authentication, data authentication, and encryption are important security methods. Analyzing worldwide adoption and supply chain management integration challenges suggests the possibility of using the BCOT model in research.

Quasar et al. [120] propose a scalable CP-ABE-based multi-agent system architecture for safe public cloud data sharing. Cloud hosts connect users and authorized agents while protecting system privacy. A new cloud malware detection method using the Gemini approach is also offered. The study improves scalability, efficiency, and malware detection, thereby enhancing CP-ABE's security, privacy, and fine granularity.

The literature survey emphasizes the potential of blockchain-based access control solutions to improve access control infrastructure investments for companies, particularly in the integration with existing systems. These solutions integrate securely and transparently with many cloud-based services and apps using blockchain's interoperability and decentralization. Integration with third-party services like identity verification providers and compliance solutions boosts blockchain-based access control systems' flexibility and extensibility. Many proposed frameworks and protocols address security and scalability issues and offer innovative approaches to data security, privacy, and access control across domains, demonstrating blockchain technology's versatility and efficacy in changing access control practices.

Enhancing scalability and performance

Sharding and horizontal scaling let blockchain networks handle increased transaction volumes by separating

data and processing transactions in parallel. Protocol enhancements, network optimizations, and consensus mechanism improvements boost blockchain transaction throughput and processing speed. Access control systems can dynamically assign resources based on demand and workload on cloud-based blockchain platforms with elastic resource provisioning and auto-scaling. Blockchain networks use load balancing to distribute transaction processing tasks evenly among nodes. It optimizes resource utilization and reduces access control system latency. This integrated method improves transaction volume control, processing speed, and system performance during variable demand.

Yan et al. [92] introduce a blockchain-based attribute-based searchable encryption data security access control system for cloud computing. The suggested method promotes fine-grained cloud data access control, secure search, policy hiding, and attribute revocation. To reduce computing costs for users, the scheme incorporates proxy encryption and decryption. Blockchain technology secures metadata ciphertext and keys and allows fair keyword searches. Smart contracts enable the dynamic monitoring of user access activity. The results demonstrate that the proposed approach enhances both storage and calculation performance while simultaneously preserving data and ensuring fair access.

Sun et al. [121] cover data security in edge-cloud collaborative applications, such as the IoTs, smart homes, and vehicles. Access control is a key technology that is being prioritized to guarantee the security of data exchange between terminals. The paper suggests hidden attribute identity authentication, which guards against identity and attribute leaks to preserve privacy. Secure data access control between terminals in various security domains and multi-domain collaborative computing in edge-cloud scenarios are made possible by intra- and inter-domain access control protocols. While safeguarding access data, a dynamic updating method for access permissions enables terminals to join or exit the system at any time. Future study areas include blockchain resource sharing, ciphertext data storage, and search.

Li and Qin [122] introduce Network Sharding Scheme (NsScheme) as a way to scale access control frameworks for IoTs blockchains. Edge nodes are sharded to maintain local blockchains, while cloud nodes manage global blockchains. NsScheme parallelizes transactions across many blockchains to increase TPS and reduce node storage. The study also provides an Access Frequency Set (AFS)-based transaction allocation system and network sharding algorithm to reduce cross-shared transaction query costs. Simulation results show linear gains in TPS with larger shard numbers.

Yu et al. [123] offered a blockchain-enhanced IIoT security access control strategy for smart factories. This blockchain-based method unifies identity authentication, public key storage, and user attribute management. User traceability and revocability ensure secure storage, access control, and information update/deletion. Evaluation results show smaller key sizes and lower overhead times than other approaches, proving IIoT security improvements.

Garg et al. [124] developed a blockchain-fog computing architecture to solve IoT security issues. For real-time applications, fog computing lowers latency, but it also presents security issues. Blockchain tackles data security breaches, access management, and user authentication. The suggested method addresses these security issues and improves fog computing IoT application security.

Imamguluyev et al. [125] propose a new node selection method for blockchain-powered edge IoT systems to reduce server load and response time. Combining fuzzy logic and TOPSIS for MCDM improves node selection efficiency and parameters. Experimental results show that this strategy optimizes node selection intervals and improves system performance.

Mallick et al. [126] suggested a new Queueing-assisted IoMT-Fog-Blockchain system to help healthcare services deal with technical issues. Temporary data processing and storage at the nearest fog node reduce overload and bandwidth requirements, improving service efficiency. Access control and patient care can be improved with queueing theory, improving system performance.

Mallick et al. [127] introduce a priority Queueing-assisted IoST-Fog-Blockchain environmental monitoring framework. This framework handles scalability, security, and interoperability issues. At the nearest fog node, the system temporarily stores, processes, and visualizes geographical data. It optimizes resource utilization and shortens service time. System performance numbers show that priority Queueing analytical methods improve access control and service delivery.

Fu et al. [128] present a blockchain-enabled device command security method for IIoT cloud platforms to solve dispersed management issues. A customizable control factor—command asset quota—limits command activities and ensures tamper-proof logs. A reference implementation project and detailed descriptions of command classification, value calculation, asset model, and quota allocation procedures are provided. Jetlinks, OceanConnect, and Fisco Bcos experiments show the scheme's feasibility, security, efficiency, and resilience.

Gai et al. [129] propose a blockchain-based Multi-signature lock for ubiquitous access controls (UACs) in the metaverse to address security concerns. All data institutions rebuild a consortium blockchain system to restrict data access. For full life-cycle data management and traceability, blockchain transaction information abstracts user data access behaviours. The proposed method has

reasonable resource usage, latency, and throughput, according to Hyperledger experiments.

Blockchain networks need scalability and performance improvements to manage higher transaction volumes, according to the research. Sharding and horizontal scalability allow blockchain networks to process transactions simultaneously, increasing throughput and speed. Dynamic resource allocation and auto-scaling enable optimal resource utilization and low latency for cloud-based blockchain access control systems. The scalability and load balancing optimisations enhance the control of transactions as well as the functionality of the system leading to more efficiency and reliability of the blockchain access control systems. In this regard, many frameworks and protocols employ the use of blockchain technology in solving security and privacy challenges in different settings, a clear indication that blockchain can transform access control and data protection.

Empowering user-centric access control

The access control systems implemented on the blockchain provides the users with the self-sovereign identity solutions where they can own their identity data. These technologies enable people to own their digital identities and this is an improvement on the concept of privacy and property in self. The other feature that the users can control includes the access policies which means that the users can make decisions on who should or should not be allowed to access specific applications. This is because access control solutions based on blockchain provide the opportunity to build a multi-level and detailed permission management system based on roles, attributes, and context. Blockchain solutions also enable users to give consent for the collection, use, and sharing of their data and also come with the ability to meet data protection laws to enhance user privacy and control.

In the same regard, Alshehri et al. [130] came up with the DSA-Block concept that enhances IoT security and privacy through secure access and data sharing. During the key generation phase, the model uses a Legitimate Device Attribute (LDA) to log user and device data. A Gateway (GW) distributes IoT device and user access requests to the edge server, allowing acceptable delegation requests. The RHSO algorithm optimizes access delegation for security, speed, and attack detection. Blockchain technology with a differential privacy mechanism encodes noise to original data to secure legitimate data in the cloud server. Off-chain storing of legal data with blockchain hash values improves security. The blockchain's PBFT consensus method speeds transaction time, block validation, and consensus. To ensure security, the model includes user attributes and user revocation procedures. The author's plans involve modifying a blockchain to improve security, processing speed, and energy efficiency during data sharing.

Qiu et al. [131] enhance a decentralized attribute-based encryption system with a more flexible threshold access structure to create a fine-grained access control mechanism for smart grids. A test phase before data decryption reduces superfluous operations and improves efficiency. Theoretical k-Linear assumptions enable adaptive security.

Song et al. [132] address IoT security issues using zero-knowledge tokens for anonymized access and increased access efficiency. The model proves IoT access control by generating and verifying zero-knowledge tokens. The study emphasizes fine-grained access control and attribute-based anonymous access due to IoT security concerns. The suggested access model addresses identity exposure and unlawful access. The study proposes a Blockchain Zero-Knowledge-Based Access Control (BZBAC) architecture to address IoT access security challenges. This safe access control architecture reduces single points of failure and credibility difficulties in traditional access models. Zero-knowledge-proof technology secures sensitive blockchain data while ensuring anonymity.

Kebande et al. [133] presented MFBC_eDS, a Blockchain-based Multi-Factor authentication mechanism, to improve Cloud-enabled IoV security. The model strengthens authentication with Security Assertion Markup Language (SAML) and single sign-on (SSO). The approach addresses authentication flaws to prevent adversarial attacks and maintain the Confidentiality, Integrity, and Availability (CIA) triad. The paper also emphasizes the significance of robust access control in connected vehicle systems and suggests future research on trust parameters and device/user attribution in IoV platforms.

Nguyen et al. [134] proposed a blockchain-based multi-user mobile edge-cloud computation offloading (MECCO) system for secure and efficient computation offloading. To protect against malicious mobile devices (MDs), they created a trustworthy access control system and a compute offloading problem. A sophisticated deep reinforcement learning technique optimised system costs and performance. Evaluation results demonstrated significant latency, energy consumption, and smart contract fee advantages over previous methodologies.

Riad and Elhoseny [135] presented a blockchain-based key-revocation access control method for safe cloud-hosted financial data and open banking. On Ethereum, they used smart contracts for key revocation. Completed experiments indicated faster response times for nonrevoked keys and acceptable data exchange rates compared to CRL and Online Certificate Status Protocol (OCSP). The approach achieved outstanding goals

like compatibility with open banking systems, protection against attacks, and efficient status response and data exchange rates.

Sohrabi et al. [136] developed a novel access control architecture to address centralized security vulnerabilities in cloud storage. They used smart contracts on a decentralized blockchain network to regulate access and reduce cloud server threats and single points of failure. They also added a master node to store decryption key components and use Shamir secret sharing to protect data. This decentralized solution improves cloud data confidentiality and prevents illegal access.

Qin et al. [137] presented a Blockchain-based Multi-authority Access Control scheme (BMAC) to improve attribute-based encryption for secure data exchange. BMAC distributes attribute management across different authorities using a permissioned blockchain and Shamir secret sharing system to reduce single points of failure. BMAC uses blockchain and smart contracts to reduce data users' communication and computation costs. It also ensures safe and auditable access management. It finishes with a security analysis and performance comparison of the suggested method.

Khatiwada and Yang [138] proposed that HS-ABE handle data privacy and availability in decentralized data storage.

This approach validates requestors according to their attributes for the security of the exchange and retrieval of information. Data owners can determine the degree of access control with the help of Ethereum, decentralized IPFS, and HS-ABE. Comparing with other related approaches, we can see that the suggested HS-ABE approach enhances the security of Blockchain-based cloud storage by managing memory effectively.

Yao et al. [139] proposed IDaaSoVCC which is an IDaaS framework for VCC with low overhead and user privacy preservation. This design adopts permissioned blockchain technology and an improved ciphertext-policy attribute-based encryption (CP-ABE) scheme to protect PII access in a distributed vehicular cloud environment. Security examination focuses on forward secrecy, confidentiality and identity information privacy, and extensive emulation demonstrates that IDaaSoVCC is both feasible and effective within large-scale distributed VC environments.

The literature review also reveals how blockchain can be used in providing self-sovereign identification solutions and enhancing the levels of privacy and control in access control systems. They allow users to manage their web persona and respective policies, enhancing privacy and data ownership. When applied to access control, the blockchain enables the precise assignment of permissions based on roles, attributes, and context information, enhancing data security compliance and user privacy and control. Several works propose creative paradigms and procedures for employing blockchain to solve security and privacy concerns in various domains, thus highlighting the versatility of blockchain and the possibility of a revolution in access control and data protection.

Promoting transparency and auditability

Each time the user demands an authentication and every time there is a modification in the authorization given, the information is stored in the public ledger of the blockchain making it possible to track the users' activities. The implementation of blockchain in access control leads to developing a system that creates an immutable record of all activities performed, which can be easily used to demonstrate compliance in case of a violation. These solutions based on blockchain also have the ability of monitoring and reporting in real time and this increases the security and the rate of response to such attacks. Blockchain also improves handling of security breaches and investigations of unauthorized access because the records are stamped for time and are not fake. This approach ensures high compliance, constant security monitoring and an instantaneous response to any event in case of blockchain-based access control solutions.

Alharbi [140] introduces the ACE-BC framework to improve data security in Critical Information Systems (CIS). A centralized blockchain-based data-sharing and administration technique overcomes security and control issues. Blockchain and the ACE-BC framework provide decentralized, encrypted data storage and access. Real-time database encryption prevents sensitive data leaks and unites the infrastructure. The system is designed for distributed storage to overcome the limitations of centralized servers and single points of failure. To address more specific access control demands, the study suggests adding ciphertext search and policy hiding based on attribute-based encryption.

Mahamuni et al. [141] suggest "Proxy Re-encryption" to secure IoT and cloud data. Identification-based encryption and the PRE model allow data owners to distribute ciphered data on the blockchain with authorized users safely. A peripheral device as a proxy server speeds computations, while information-based networks increase service. Decentralized data sharing using blockchain technology reduces the limits of centralized systems and ensures strong access control, integrity, and confidentiality.

Ravi et al. [142] highlight the problems of conventional healthcare systems enhanced by IoT growth. Patients' data is transferred securely using blockchain technology based on their authorized settings, maintaining privacy. In IoT, a blockchain-based privacy protocol protects user data from rogue cloud servers. Evaluation and

experimental results show that smart contracts enforce security standards and data privacy for multi-sharing adjustable access control, proving their efficiency and applicability.

George and Chacko [143] proposed MediTrans, a blockchain-based patient data access management system, to address patient-centric medical information control. Patients save treatment data in a secure personal health record (PHR) cloud, allowing controlled access to healthcare professionals. MediTrans secures data transport and access via blockchain and attribute-based encryption. Promising results for practicality were obtained from an Ethereum Blockchain prototype tested with OpenEMR.

Li et al. [144] introduced a blockchain-based scheme called BPRPDS to address issues regarding privacy. It also provides incentives for the exchange of private data by IoTs devices. BPRPDS prohibits behaviour profile construction and nonframeability with Monero and deniable ring signatures. Smart contracts allow flexible multi-sharing access. The method is secure and efficient, according to the performance study.

Kang and Kim [145] present the Health Care Big Data Platform (HBDP), a safe healthcare research platform that addresses eHealth data privacy concerns. HBDP provides fine-grained access control, safe storage, and accountability using attribute-based encryption and private blockchain. Case studies confirm the platform's viability and security by demonstrating illegal user detection, and empirical evaluations show efficient data encryption and blockchain performance. HBDP is a secure and private approach for using eHealth data in research.

Du et al. [146] present a blockchain-based Privacy-Preserving Searchable Encryption (PPSE) method to mitigate cloud outsourcing data alteration and leakage threats. Security, query performance, and storage overhead are improved by keeping encrypted indexes in a private blockchain and encrypted documents in a public blockchain. Secondary verification access control with smart contracts ensures data privacy and accuracy. Safety research and experimental findings show that blockchain storage eliminates third-party verification and produces correct and unchangeable data.

Zhang et al. [147] propose a method that makes use of white-box tracking and alliance chains to overcome the difficulties of security and privacy that are associated with the exchange of data in the Internet of Things. The goal is to identify malicious users, eliminate dependency on a central authority, and safeguard user privacy through blockchain anonymity. Multiauthority environments and consensus nodes maintained by diverse authorities improve security and performance. The proposed system is better than comparable ones based on security analysis and simulation findings.

According to the literature review, blockchain-based access control solutions can improve security, compliance, and incident response. Public blockchain ledgers automatically record authentication requests and authorization modifications, enabling immutable audit trails for regulatory compliance audits. Blockchain technologies facilitate monitoring and reporting in real-time to identify threats in advance and act on them as soon as they are detected. Blockchain systems also store the original and time-stamped ACEs for the forensic study as well. The blockchain-based access control systems are very crucial in the modern cybersecurity since they provide strict compliance, real-time security monitoring, and proper management of security threats. In addition, the research also provides new solutions and approaches based on the blockchain technology to solve specific security and privacy challenges in different domains, which also confirms the prospect of blockchain in improving data security, privacy, and access control.

Enhancing security with multi-factor authentication

Due to the nature of public blockchains being append-only, they record access control events, for example, authentication or permission modification. These provide a fixed and open record of user activities and this is very crucial. Blockchain based access control solutions have the added advantage of providing a record of all the activity that takes place in an organization and this is especially useful when it comes to proving compliance with regulations during an audit. Blockchain-based solutions also provide real-time monitoring and reporting, improving security and enabling quick reaction to threats. Blockchain technologies also ease forensic analysis and incident response by providing exact and time-stamped access control event records. Businesses using blockchain-based access control systems benefit from this integrated approach to compliance, security monitoring, and incident response.

Yang et al. [148] examine security challenges in blockchain and cloud systems, emphasizing the lack of blockchain research on cloud privacy protection and access control difficulties. Traditional cloud access control relies on trusted centres and administrators, making it vulnerable to internal and external threats. The paper introduces AuthPrivacyChain, a privacy-focused access control architecture, to prevent cloud attackers from accessing resources. The EOS blockchain is used to record all authorization-related transactions in this architecture. Access authorization and related information are added descriptors in blockchain transactions.

Pandiaraj et al. [149] suggest a secure, decentralized blockchain for medical data stored in the cloud as

a solution to security and privacy issues in electronic health records. Healthcare providers exchanging patient health data benefit from enhanced network security, data privacy, and confidentiality thanks to blockchain technology. In comparison to a prior data-sharing paradigm, the study demonstrates better lightweight access control, decreased network latency, and greater security and privacy. It provides a resilient mobile data transfer technique.

Verma et al. [150] propose using blockchain and fog computing to secure cloud-connected healthcare IoT devices. Existing systems are vulnerable. Thus, they suggest homomorphic encryption, safe access control, and distributed data management. This method enhances patient health data transfer security and privacy while improving autonomy and adaptability over existing models. The research addresses major digital healthcare sector issues and proposes a secure data management and access control architecture for Personal Health Record (PHR) systems.

Chinnasamy et al. [14] suggest a smart contract and blockchain-based access control solution for secure healthcare data exchange. Cloud-based healthcare data-sharing applications have trust issues with third-party suppliers, pushing blockchain adoption to reduce dependency. The proposed technique enhances security while facilitating the patient-physician exchange of electronic health records for sensor-generated data streams. In mobile computing, smart contracts provide proactive resolution for secure data transfer, lowering risks and increasing usefulness, network performance, and data concealment.

The literature review shows how blockchain-based access control solutions improve security, privacy, and compliance in cloud-connected healthcare systems. Immutable and transparent audit logs of user activity on public blockchain ledgers let organizations demonstrate regulatory compliance during audits. They help in threat identification and incident management by continuously monitoring and alerting the technologies. Moreover, blockchain systems give the precise and time-stamped records of access control event for investigations. To enhance the security of the network and to avoid intruders to access the resources in cloud, researchers suggested the implementation of access control solutions based on the blockchain, for example, AuthPrivacyChain. Safe distributed cloud based medical blockchains are better to implement than the traditional data sharing paradigms and provide lightweight access control, low latency, and enhanced security and privacy. Together, they can greatly alter the methods of protecting data in the current and future states of healthcare systems and access to them.

Facilitating regulatory compliance and reporting

It can also help organizations that are dealing with data protection laws such as General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) through the use of blockchain-based access control. They assist in satisfying the need for the regulations by having good access controls, reporting and recording features, and data protection measures. Chain-based access control systems produce a lot of records of access control activities, change in policies and user engagements that may be useful during audits and reviews to show compliance. Therefore, the access control data is written in a non-editable form, and this implies that audit trails and compliance records cannot be modified. Furthermore, blockchain-based access control systems comply with the legal and regulatory standards defined by industry bodies or International Standards Organizations. It also enhances the standards of governance and risk management hence enhancing the confidence of the stakeholders.

Sharma and colleagues [151] propose a structure based on blockchain that allows limited access to external users to maintain privacy and security in cloud storage. For user revocation the algorithm used is the CP-ABE which reduces the dependency on a single authority and scale. Hence from the analysis it is concluded that the proposed architecture is more scalable and efficient to address the privacy issues related to the outsourced cloud data through efficient administration.

Li et al. [152] present OLOS, a hybrid on-chain ledger, and off-chain storage EMRs management paradigm, to address blockchain-enabled healthcare service systems (HSS) problems. Reducing ledger corpulence and enhancing data security, OLOS keeps actual data on local servers and publishes EMR indexes to the public blockchain. To safeguard cross-institutional EMR sharing, they additionally provide keyword-searchable attribute-based encryption (KS-ABE) techniques based on lattice cryptography. Compared to similar initiatives, it resists quantum assaults with reduced transmission costs and key sizes.

Jayatunga et al. [153] highlight the necessity for reliable vehicle communication networks as 5G and 6G arise. Traditional V2X communications fail to fulfil changing needs, causing participant distrust. Blockchain integration would assure network integrity and accountability. Blockchain and 5G Multiaccess Edge Computing (MEC) are also investigated to improve security and efficiency in V2X networks and solve data privacy leakage and cyberattacks.

Li et al. [154] propose blockchain-based searchable encryption access control to secure IoT data sharing. This solution uses blockchain's decentralization and tamper-proofing to search encrypted data securely. Restricting

cloud access to privacy-related data ensures privacy. Simulated data encryption, decryption, and searching require 33%, 5%, and 75% less time than current approaches.

Deebak and Hwang [155] introduce a cloud-based healthcare application to solve data sharing and decision management privacy problems. To ensure data preservation and privacy, its cloud-assisted decentralized privacy-preserving framework (CA-DPPF) makes use of blockchain technology and key agreement methods. The scheme meets healthcare supply chain management security requirements for conditional traceability and data integrity through rigorous security analysis. Exploration shows that CA-DPPF improves transaction efficiency by reducing latency and increasing throughput to maximize service use.

Nguyen et al. [156] suggest a unique architecture for sharing EHRs that combines blockchain technology and IPFS on mobile cloud platforms. Secure EHR sharing between patients and doctors is achieved with smart contract access control. A real-world Ethereum blockchain prototype shows secure data exchanges for health information. A lightweight access control approach with reduced network latency and improved high-security performance over traditional models is shown via system evaluation.

Wang et al. [157] suggest a blockchain-based EHR sharing protocol for security and privacy. Blockchain's anonymity and decentralization address data security and privacy. Conditional proxy re-encryption and searchable encryption provide data protection and access management. Consortium blockchain consensus relies on proof of authority to ensure system availability. Security research proves the protocol works, while Ethereum performance evaluation shows good computational efficiency.

The literature review emphasizes the importance of access control solutions based on blockchain in GDPR and HIPAA compliance. These technologies enforce strict access rules, create detailed audit trails, and protect data integrity to improve compliance. Blockchain-based access control systems ensure audit trails and compliance records are tamper-proof, building stakeholder trust. These systems also meet industry-specific regulatory authorities' or worldwide standards organizations' regulatory criteria, improving governance and risk management. Additional research suggests innovative blockchain-based approaches to privacy and security issues in cloud storage, healthcare service systems, vehicle communication networks, IoT data sharing, and electronic health record management, demonstrating blockchain's versatility and potential to secure, privacy, and comply with data across diverse domains.

Empowering edge computing and IoT devices

Edge computing nodes effortlessly integrate access control techniques for safe authentication and authorization of IoT devices and edge applications at the network edge, closer to the data source. Blockchain-based access control systems protect IoT data by encrypting data transmissions, authenticating devices, and implementing access policies at the network edge. In edge computing contexts, lightweight access control protocols like MQTT and CoAP provide quick IoT device authentication and authorization despite limited resources and bandwidth. Blockchain systems authenticate and authorize IoT devices and edge applications at the network edge using decentralized identity solutions, cryptography, and consensus processes. It enables safe and efficient edge computing access management. This integrated approach improves IoT security and resilience, boosting edge computing trust and reliability.

Al Breiki et al. [158] suggest a decentralized Internet of Things data access management system built on blockchain and using trusted oracles. End users may have decentralized access control over remotely stored IoT data thanks to smart contracts. Blockchain networks and IoT data hosts are connected via trusted oracles. The method enables end users and DApps to choose reliable oracles by using smart contracts to create a decentralized Oracle reputation service. The author plans to use cloud-stored IoT data to create a fully working system. He created frontend DApps for participant engagement and software for trustworthy oracles to access the data and communicate with Ethereum smart contracts. This implies real-world development and use of the suggested decentralized access control technology.

Pateritsas and Petrakis [159] described iBoT, a blockchain-based cloud IoT platform, highlighting its security and WoT concepts. The private blockchain of iBoT uses Hyperledger Fabric to securely identify users, devices, and apps. Subscriptions and a Gateway service that monitors blockchain events set iBoT apart. Credential security and latency can be improved to satisfy real-time IoT requirements.

Bisht et al. [160] suggest merging blockchain with edge computing to improve scalability and decentralized resource control. They analyze the problems and offer a new SC-IBEC architecture to optimize consensus processes and scalability for this integration. To better blockchain-edge computing fusion, current issues are addressed and future solutions are proposed.

EdgeShare is a blockchain-based solution that enables secure data exchange in the Industrial Internet of Things (IIoT), according to Yang et al. [161]. It provides solutions for scale and security issues. Data-sharing efficiency is increased using an edge computing paradigm and a two-layer overlay network design. Blockchain-based access

control methods with varying granularities for transaction recording and auditing are made possible by a novel smart contract. Comparisons to centralized systems show increased reliability, efficiency, and security, with large-scale node tests in real industrial scenarios planned for optimization.

Fugkeaw et al. [162] offer the LightMED access control scheme for safe and scalable cloud-based EMR sharing using fog computing, CP-ABE, and blockchain technology. The system tackles outsourced encryption, IoT data transmission, and EMR policy updates security and privacy concerns. LightMED offers a lightweight policy update mechanism, outsourced encryption with a privacy-preserving access policy, and secure IoT data transfer and aggregation. Experimental results show the scheme's efficiency and practicality compared to previous works.

Ma et al. [163] suggest a blockchain-based BDKMA for IoT hierarchical access control to solve decentralization, auditability, scalability, and privacy. Cloud-stored multi-blockchains and side blockchains, managed by SAMs in each domain, enable interaction between domains. Simulations show better system performance and scalability. Future work will create a SAM and cloud management feedback mechanism to improve blockchain-based IoT ecosystem persistence.

The examination of the literature indicates significant advancements in the integration of edge computing with blockchain technology to enhance the security and effectiveness of Internet of Things systems. Edge computing nodes are adding access control techniques for safe authentication and authorization near the data source. IoT data at the network edge is secure with blockchain-based encryption, decentralized identification systems, and consensus mechanisms. MQTT and CoAP are lightweight protocols that speed up authentication and authorization despite resource limits. Al Breiki et al. [158] decentralized IoT data access control system employing trusted oracles, Pateritsas and Petrakis' [159] Hyperledger Fabric-based iBoT platform, and Bisht et al.'s [160] SC-IBEC architecture demonstrates scalability and decentralization. Yang et al.'s [161] EdgeShare and Fugkeaw et al.'s [162] LightMED systems improve industrial and medical data-sharing efficiency and privacy. Ma et al.'s [163] BDKMA platform handles cross-domain interactions and scalability issues, looking for potential for blockchain-integrated edge computing ecosystems. These studies show that blockchain can improve edge computing IoT security, scalability, and reliability.

Enabling transparent supply chain management

Blockchain ledgers record product shipments, deliveries, and inventory transfers in an immutable and transparent manner. It makes the history of transactions and item movement within the supply chain network visible. In supply chain management systems based on blockchain, suppliers keep track of the procurement of raw materials through production, delivery, and distribution by gathering and documenting information. Blockchain-based access control solutions enforce access controls, document compliance, and provide audit trails for regulatory bodies, assuring supply chain compliance with product safety and import/export regulations. Blockchain systems provide transparent access to supply chain data. It allows regulatory agencies, auditors, and stakeholders to verify compliance, investigate concerns, and track product and material origins seamlessly across the supply chain network.

Li et al. [164] IoT logistics data is encrypted and collected into a customized blockchain structure for security and fine-grained access control. We also develop an efficient consensus approach to improve consensus process efficiency. Simulation results show Logisticschain's efficacy and practicality. However, future research should evaluate logistics providers' reputations.

Jayasri et al. [165] presented a progressive temporal blockchain-based Secure eHealth Framework (SeFra) to solve healthcare scalability, usability, and accessibility. CBMT and CBAC improve security and integrity verification in SeFra. Temporal features, HL7 protocols, and IPFS data management address interoperability and scalability difficulties. SeFra secures the Personalised Micro Ledger (PML) and distributes medical data while adhering to context-based smart contract limits.

Zheng et al. [166] suggested a blockchain-based model to fix problems with credit data in the supply chain financial credit system. The model would focus on honesty, freedom, openness, safety, and dependability. A consensus mechanism for massive credit investigation data and privacy protection is used with proxy re-encryption for cloud server data storage. To promote credit information exchange and consensus efficiency, the model incorporates the RPBFT consensus method. The practical ramifications include improving decentralized transactions, trustworthy transactions, and data security and privacy. Testing and validating the framework, governance structures, and interdisciplinary collaborations to improve public knowledge and application value of blockchain technology are future research prospects.

Noh et al. [167] developed a blockchain-based data integrity auditing protocol for South Korea's smart HACCP system to overcome centralized access control's drawbacks and ensure reliability. The technique verifies cloud server data integrity without downloading the source data using a Merkle Hash Tree (MHT), enhancing computing performance. Qualitative investigation shows that the protocol meets smart HACCP system requirements with low computational overhead.

Han et al. [168] offer a modified EOSIO blockchain and IPFS distributed storage peer-to-peer data storage and sharing solution to solve centralized cloud service provider problems. Hybrid encryption protects data and allows various uses and persistent storage. The blockchain component is expanded to offer customizable transaction auditing. System analysis and experimental evaluation indicate good performance and large on-chain storage usage savings, proving availability and scalability.

Qureshi et al. [169] propose a Blockchain-based Privacy-Preserving Authentication (BPPAU) model for ITS to address privacy and security issues in centralized infrastructures. BPPAU stores, accesses, and processes data using blockchain smart contracts, access control mechanisms, and on-demand operations. Simulated performance includes transaction cost analysis, transactions per second with block time, and computational time analysis with many transactions to prove the model's efficacy.

Li et al. [170] present a blockchain-based fine-grained VANET data access management method for security and privacy. FADB uses blockchain to manage user identities and store data, assigning access permissions based on attributes. Enhanced CP-ABE lets lightweight VANET devices outsource encryption and decryption to RSUs, boosting data access. Computer simulations and security research show that FADB secures data with negligible performance overhead.

Blockchain technology may enhance security, privacy, and efficiency in supply chain management, logistics, healthcare, and data integrity checks, according to the studied literature. Li et al. [164] The logistics chain uses simulations to demonstrate its encrypted, customized blockchain structure for cloud storage privacy. Zheng et al. [166] use a robust consensus mechanism to increase supply chain finance trust and data privacy, whereas Jayasri et al. [165] use temporal blockchain and IPFS to scale healthcare. Merkle Hash Trees helps Noh et al. [167] verify smart HACCP data integrity reliably and efficiently. Han et al. [168]offer scalable and secure peer-to-peer data storage with hybrid encryption. Qureshi et al. [169] BPPAU's approach for ITS uses blockchain smart contracts for privacy-preserving authentication and performs well in simulations. Finally, Li et al.'s [170] FADB VANET data access management solution uses upgraded CP-ABE for secure, low-overhead data handling. various studies recommend validation, scalability enhancements, and interdisciplinary collaborations to fully realize blockchain's benefits in various applications.

Supporting immutable digital identities

A blockchain ledger records user profiles, credentials, and certifications in an immutable manner, ensuring their authenticity and permanence. Identity management systems use blockchain technology to create portable and interoperable identity credentials. These can be securely shared and verified across platforms, applications, and organizations, enabling seamless identity management and eliminating reliance on centralized providers. Blockchain-based access control systems authenticate and verify users' identities safely and transparently using decentralized identity solutions, cryptography, and consensus procedures. In supply chain management systems based on blockchain, suppliers keep track of the procurement of raw materials through production, delivery, and distribution by gathering and documenting information.

Guo et al. [171] provide a novel way to decentralize authentication, authorization, and auditing responsibilities through the utilization of blockchain technology. The transparent blockchain preserves auditing data, preventing impersonation, collusion, and manipulation. The performance analysis highlights the solution's efficient transaction-related computations.

Ri et al. [172] introduce a blockchain-based Role-Based Access Control (RBAC) architecture with Separation of Duties (SoD) constraints and a cloud-based access control system. The proposed access control approach confirms role ownership using a user-generated keypair of private and public keys and manages access requests through their model. An Ali cloud environment simulation shows that the approach improves security and access control by integrating Separation of Duties (SoD) requirements on the blockchain.

Almasian et al. [173] propose a blockchain-based cloud storage access control architecture for fast revocation. The architecture uses public blockchain and cloud service models to solve storage, accessibility, and backup issues for businesses without a trusted element. The blockchain connection allows financial transaction outsourcing and denial-of-service protection. Public blockchain systems with smart contracts may improve web application security and service. Smart contracts prevent centralization and single points of failure in access control frameworks, unlike conventional methods that may be insecure and difficult to maintain.

Saini et al. [174] presented a blockchain-based smart contract access control framework for healthcare system's electronic medical records (EMRs). Four smart contracts are introduced for user verification, access authorization, misbehaviour detection, and access revocation. EMRs are encrypted using ECC and kept in the cloud, while their hashes are in the blockchain. The suggested framework for real-time smart healthcare systems is efficient when tested on a private Ethereum system.

Naresh et al. [175] proposed DPEM, a decentralized healthcare system that prioritizes reliability, privacy, security, and trust to combat escalating data breaches. DPEM's four-layer structure uses blockchain and elliptic

curve-based content extraction signature to protect privacy, secure data exchange, and control access. DPEM uses blockchain smart contracts and CP-ABE to secure storage, data sharing, and access control while ensuring responsibility and integrity. DPEM is optimized for secure EMR data transfer, according to security studies.

Ding and Sato [176] presented Bloccess, a framework for fine-grained access control that makes use of a permission blockchain. To address trust difficulties in contexts that are not trustworthy, such as the Internet of Things (IoT). Bloccess improves dispersed access control management with a single, user-centric approach. The danger model states that optimizing decentralized access control secures protected settings. Security study and comparison with relevant frameworks confirmed feasibility and efficacy.

Chen et al. [177] proposed a blockchain-based medical data exchange method to address sensitivity and centralization. The technique protects data with K-anonymity and searchable encryption. Medical records are protected and secured using Hyperledger Fabric, a consortium blockchain. Security and performance assessments prove the solution's viability and efficacy.

Doshi and Khara [178] prototyped a multiuser access control approach to secure cloud data against hostile actors. The system controls access without provider participation using ciphertext policy attribute-based encryption with dynamic characteristics. The technology secures sensitive processes with hashed codes and a decentralized ledger that records security occurrences immutably. To prove its efficacy, the smart contract prototype was tested.

Jabarulla and Lee [179] presented an Ethereum blockchain and IPFS proof-of-concept design for distributed patient-centric image management (PCIM). This method protects patient data without centralization. PCAC-SC smart contracts authorize patients to control their medical imaging data access on the blockchain. Experimental implementation demonstrated efficient and feasible, enabling public blockchain deployment and AI integration for better diagnosis.

According to the literature review, blockchain technology can transform access control and identity management across various sectors. Blockchain's immutable ledger verifies and secures user credentials, making identity management systems portable and interoperable. Decentralized identity solutions, cryptography, and consensus methods improve user authentication and access control security and transparency. Guo et al.'s [171] decentralized authentication model, Ri et al.'s [172] RBAC architecture with SoD limitations and Almasian's [173] Rapid cloud storage revocation design is a notable contribution. Other creative frameworks, including Saini et al.'s [174] smart contract-based access control for healthcare, Naresh's [175] DPEM for safe EMR data transfer, and Chen's [177] medical data exchange technique demonstrate blockchain's significance in security, privacy, and trust. These studies show that blockchain may solve traditional security problems, optimize access control, and manage sensitive data. To fully utilize blockchain's secure and efficient access control features, further research should improve scalability, usability, and interface with existing systems. Table 6 explains some prime research among all the 12 sub-categories for blockchain-based access control, along with their issues and solutions.

Applications of blockchain-based access control in cloud environment

In this section, we will explain the different scenarios where blockchain based access control for cloud can be applied and how this innovative technology is being implemented across different fields to improve productivity, responsibility and security of the cloud environment. Beginning with banking and insurance industries, followed by healthcare and pharma, we will explore how the technology is reshaping the operational processes and data. Furthermore, we will also find out how it affects public sector services, infrastructures, and supply chain, technology and DevOps, and enterprise resource planning. Figure 10 shows important applications in this area.

Healthcare

Blockchain-based access control is revolutionizing the administration of sensitive data and operational processes in the healthcare sector [109]. One can safely assume that only those who are supposed to, in this case, the authorized medical personnel, should be able to view or modify the information about a specific patient, making it secure for use in the management of patient records in the healthcare industry. This also improves compliance with regulatory needs such as the Health Insurance Portability and Accountability Act (HIPAA) and data privacy [104]. The application of blockchain in telemedicine will also serve to protect the virtual consultations from unauthorized access and the patients' data from unauthorized disclosure. Blockchain technology enables the protection of data during sharing, which is advantageous to medical research. This technology allows only authorized researchers to access sensitive data which assists in promoting teamwork and at the same time ensures that data is not compromised [98]. Additionally, improvements are observed in prescription management, as blockchain technology guarantees that prescription data is accessible only to authorized prescribers and pharmacies, thereby minimizing fraud and abuse. In the pharmaceutical sector, blockchain technology improves the security of the drug supply chain by enabling end-to-end visibility and access control, thereby preventing the introduction of

Table 6 Some of the key researches with their issues and solutions

Reference	Issue	Solution	Key Focus
[86]	Challenges in traditional cloud storage systems.	Decentralized storage technologies (IPFS) integrated with Ethereum blockchain and ABE.	Fine-grained access control, test case studies, and future improvements in attribute revocation.
[79]	Security challenges in cloud-based big data storage	Blockchain-based verifiable user data access control policy	Privacy protection, unique node IDs, and ongoing research for evolving application requirements
[87]	Fairness and reliability in searchable encryption	ABSE scheme with blockchain, introducing reward and punishment mechanism	Economic consequences, incentivizing honest behaviour, and addressing index structure flexibility
[88]	Authentication and access control in Mobile Cloud Computing (MCC)	Auditable and privacy-preserving authentication using blockchain.	Dynamic pseudonyms, efficient access permission updates, and exploration of efficiency improvements.
[100]	Cloud storage access control security.	Blockchain-based access control framework	Modified ciphertext-policy ABE algorithm, decentralized distribution key, and exploration of decentralized storage platforms.
[92]	Data security access control in cloud computing	Blockchain and attribute-based searchable encryption	Fine-grained access control, secure search, policy hiding, and attribute revocation.
[112]	Data privacy in Supply Chain Management (SCM).	Blockchain-based ABAC model.	Two-tiered network design, scalability, and efficiency optimizations.
[140]	Data security in Critical Information Systems (CIS).	ACE-BC framework is decentralized and has encrypted data storage.	Outperformance, future functionalities, and exploring applications.
[148]	Security issues in blockchain and cloud systems.	AuthPrivacyChain framework	Confidentiality, integrity, availability, authenticity, and accountability.
[90]	Privacy-preserving access control in IoT environments	CapChain framework	Reliability, scalability, and suitability for IoT
[158]	Decentralized access control for IoT data.	Blockchain and trusted oracles	Decentralized access control, reputation service, and system implementation.
[180]	QoS and security in cloud environments	Integration of IP-based authentication, threat analysis, and blockchain-based Group Whale Optimization.	Validation under different cloud deployments, integration with deep learning methods.
[130]	Dynamic secure access and data sharing in IoT	DSA-Block model, utilizing blockchain	Consortium blockchain, PBFT consensus algorithm, and attack mitigation.
[131]	Fine-grained access control in smart grids.	Decentralized attribute-based encryption scheme	Privacy budgets for trajectory data.
[91]	EHR security concerns	C-AB/IB-ES scheme using blockchain.	Integrity and traceability, deploying smart contracts, and exploring additional applications.
[121]	Secure data sharing in edge-cloud collaborative scenarios	Identity authentication and access control based on hidden attributes	Access control algorithm efficiency and exploration in IoT and medical data security.
[132]	IoT access control	Blockchain Zero-Knowledge-Based Access Control	Efficiency enhancement and deployment in diverse security contexts.
[173]	Fast revocation in cloud storage	Blockchain-based access control framework	Public blockchain integration, scalability, and application in EHRs.
[171]	Decentralized authentication, authorization, and auditing for cloud data	Blockchain-based approach	User attribute revocation and scalability.
[172]	RBAC model with SoD constraints for cloud environments	Blockchain-based RBAC model.	Refining for improved response time and scalability
[151]	Privacy and security in cloud storage	Fine-grained access control using blockchain and CP-ABE.	Integrity checking mechanisms and distributed payment systems.
[181]	Cloud security through blockchain-based access control	Blockchain-based access control and data sharing approach.	Optimization in access control and data sharing, potential applications in cloud storage.

counterfeit drugs into the market [97]. It simplifies the management of clinical trials by protecting the integrity of trial results, guaranteeing regulatory compliance, and securely managing access to trial data.

Enterprise resource management

Across a variety of sectors, blockchain-based access control considerably improves operational efficiency and enterprise resource management. It guarantees supply chain transparency in retail and e-commerce by regulating data access at each stage, from manufacturing to dispatch, thereby enhancing trust and reducing fraud [182]. Additionally, customer data privacy is enhanced, enabling customers to regulate the access to their personal information, thereby fostering compliance with data protection regulations and fostering trust [35]. In

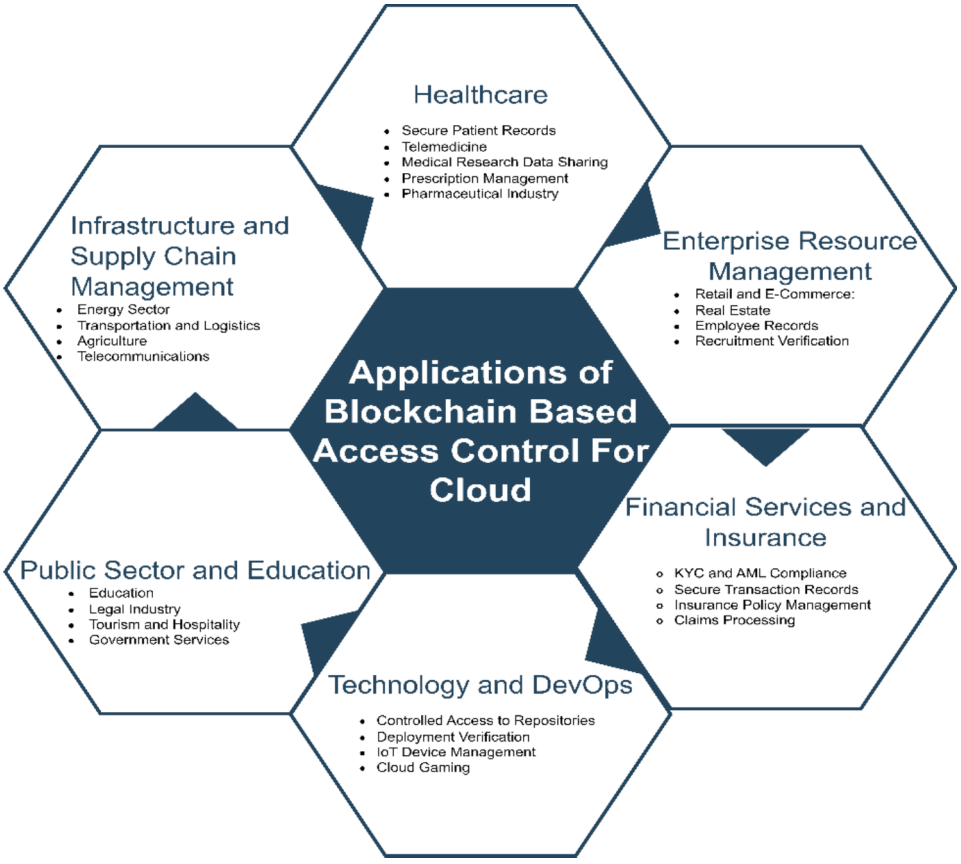

Fig. 10 Applications of blockchain-based access control specifically in cloud environment

the real estate sector, blockchain technology secures property title administration, preventing title fraud by ensuring that only authorized parties can access and modify ownership records [183]. Smart contracts facilitate automated enforcement of rental agreements, guaranteeing transparency and compliance [45]. Blockchain technology is employed by human resources departments to maintain the security of employee records, guaranteeing that only authorized personnel have access to sensitive information. Verifying applicant credentials and employment history on the blockchain streamlines recruitment processes, thereby enhancing recruiting efficiency and reducing fraud.

Financial services and insurance

Security, compliance, and operational effectiveness are all getting better with blockchain-based access control in the financial services and insurance industries. Financial institutions utilize blockchain technology to ensure KYC (Know Your Customer) and AML (Anti-Money Laundering) compliance [184]. This technology simplifies regulatory compliance and audits by securely managing and verifying customer identities and recording each verification step immutably. The blockchain is used to maintain secure transaction records, which provide transparent and tamper-proof documents that aid in the detection and prevention of fraud, as well as the maintenance of regulatory compliance [185]. In the insurance sector, blockchain improves policy administration by regulating access to policy data, ensuring that only authorized agents and policyholders can view or update information [91]. Blockchain streamlines claim processing by automating claims approval and payment through smart contracts, which ensure that only verified claims are processed. This reduces fraud and improves efficiency.

Technology and DevOps

Blockchain-based access control improves security and operational integrity in the DevOps and technology sectors. Blockchain technology regulates access to code repositories in DevOps and CI/CD pipelines, guaranteeing that only authorized developers are permitted to make modifications and guarantee a transparent, tamper-proof history of modifications [186]. To guarantee that only code that has successfully passed the necessary tests and approvals reaches production, deployment verification is automated through smart contracts. Decentralized authentication is advantageous for IoT device administration, as it guarantees that only authenticated devices communicate with cloud services [185]. This is achieved

by registering each device on the blockchain. The blockchain is used to administer secure firmware updates, ensuring that only authorized updates are deployed. Each update is logged for transparency. Blockchain is responsible for user authentication in cloud gaming, guaranteeing that only authorized participants have access to in-game assets and games. It also ensures the secure management of in-game assets by enforcing ownership and transfer rules through smart contracts, thereby providing transparent transaction histories that prevent fraud.

Public sector and education

In education and government, blockchain-based access control improves security, transparency, and efficiency. In the field of education, blockchain technology is used to safeguard student records, ensuring that only authorized personnel can access or amend academic information [187]. This enhances privacy and ensures that data protection regulations are adhered to. Credential verification is facilitated by the issuance and verification of educational credentials via blockchain technology, which ensures authenticity and streamlines the verification process for employers and other institutions. Secure document management is advantageous to the legal sector, as it regulates and records access to confidential legal documents on the blockchain. Smart contracts guarantee transparency and compliance by automating and enforcing legal agreements. [188] Blockchain technology improves the privacy of visitor data in the tourism and hospitality industry by controlling access to personal information, ensuring that only authorized personnel can view or modify it. Blockchain technology ensures the security of reserving systems, ensuring that booking records are transparent and unalterable. The integrity of elections is guaranteed by the use of blockchain technology in government services, including voting systems, to ensure secure voter authentication and tamper-proof voting records. Blockchain simplifies regulatory reporting and guarantees transparent, immutable audit traces, further enhancing compliance in financial services.

Infrastructure and supply chain management

Access control that is based on blockchain technology improves operational efficiency, transparency, and security in the administration of infrastructure and supply chains. In the energy sector, blockchain controls access to smart grid data, guaranteeing that only authorized personnel and devices can interact with the grid, thereby improving security and efficiency [166]. Blockchain technology is implemented by energy trading platforms to verify and authenticate participants, thereby guaranteeing transactions that are both transparent and secure. Blockchain enhances operational efficiency by controlling access to vehicle and route data, ensuring that only authorized personnel can update information, thereby securing fleet management in transportation and logistics [112]. Blockchain technology has also enhanced cargo tracking by assuring the authenticity and integrity of shipment data by providing secure and transparent information. In agriculture, blockchain oversees access to farm data, guaranteeing that only authorized users can view or amend the information, thereby improving data security and transparency. For agricultural supply chains, blockchain's transparency is advantageous because it regulates access at every level to prevent fraud and guarantee the product's authenticity [15]. In the telecommunication industry, the blockchain is employed to control the connection to the networks that are only to be utilized by authorized devices and users for security purposes. Further, by incorporating the use of blockchain technology in the management of the customer data, the personal information of the customers is safeguarded and the access to the data is controlled to meet the requirements of the data protection laws.

Conclusion and future research directions

In conclusion, this review article has discussed and assessed the integration of access control and blockchain in the context of cloud computing. To gain the necessary insights into the variety of blockchain-based access control systems, we gathered 118 papers from various academic databases and divided them into 12 different clusters. Based on the literature review, we found out that blockchain can improve access control by providing a secure, decentralized and tamper-proof solution. Despite the promising prospects, there are still difficulties that need to be addressed, such as scalability, interoperability, and security, which indicates that additional research and development efforts are required. However, the examined literature suggests that blockchain is becoming more widely recognized as a viable means of improving security and instilling trust in cloud systems. Researchers and practitioners must collaborate to address existing challenges and advance the current state of blockchain-based access control.

Numerous challenges are identified in this study, and future research directions are suggested for this rapidly emerging area, as discussed in Table 7. One of the primary challenges is the scalability of blockchain networks, as the increasing volume of transactions can result in high processing costs and latency. Which in turn affects the efficacy of access control systems. Blockchain integration with cloud infrastructures also causes compatibility and interoperability concerns. The public ledger storage of sensitive access control data raises privacy problems. Future research should develop more scalable and efficient consensus algorithms, explore hybrid blockchain systems with public and private aspects, and

Table 7 Major challenges associated with Blockchain-based access control with future research direction and the possible solution for these future research direction

Sr.	Challenges	Possible Solutions	Future Directions
1	Scalability issues due to increasing transaction volume and network congestion	• Integration of off-chain protocols like state channels and sidechains • Utilization of off-chain scaling solutions such as state channels and plasma chains • Deployment of parallel processing techniques and distributed ledger partitioning	• Implementation of sharding techniques and layer-2 scaling solutions • Implementation of advanced consensus algorithms like proof-of-stake (PoS) and DAG-based approaches • Research into novel consensus mechanisms such as asynchronous Byzantine fault tolerance (ABFT)
2	Security concerns regarding data privacy and confidentiality	• Adoption of robust encryption standards and decentralized identity solutions • Adoption of privacy-focused blockchain platforms and decentralized identity management systems • Adoption of blockchain-based data encryption and secure data-sharing protocols	• Advancements in cryptographic techniques such as zero-knowledge proofs • using cutting-edge methods for protecting privacy, such as secure multi-party computing (MPC) and homomorphic encryption • Advancements in privacy-enhancing technologies like zk-SNARKs and ring signatures
3	Interoperability challenges among different blockchain platforms and cloud systems	• Employment of interoperability bridges and middleware solutions • Deployment of interoperability middleware layers and blockchain gateways • Development of cross-chain interoperability frameworks such as Polkadot and Cosmos	• Development of cross-chain communication protocols and interoperability standards • Development of universal interoperability protocols and cross-platform smart contract standards • Standardization of APIs and protocols for seamless integration between blockchain networks and cloud platforms
4	Regulatory compliance complexities in a global cloud environment	• Collaboration with regulatory bodies to establish compliance guidelines • Utilization of smart contracts for automated compliance enforcement and auditing • Integration of regulatory compliance modules within blockchain smart contracts	• Emergence of regulatory frameworks tailored for blockchain in cloud computing • Formation of international regulatory bodies and cross-border compliance frameworks • Implementation of self-sovereign identity solutions and decentralized compliance verification mechanisms
5	Lack of standardization in access control mechanisms across blockchain networks	• Adoption of open-source access control frameworks and protocols • Implementation of smart contract-based access control policies and decentralized identity solutions • Adoption of decentralized access management platforms utilizing blockchain-based authentication	• Establishment of industry-wide standards for access control in cloud-based blockchains • Creation of industry consortia for access control standards development • Development of blockchain interoperability standards for access control policies and permissions
6	Performance overheads associated with executing smart contracts in cloud-based blockchains	• Utilization of off-chain computation networks and execution layer optimizations • Integration of layer-2 scaling solutions like sidechains and rollups for enhanced throughput	• Optimization of virtual machine execution environments and gas fee structures • Optimization of smart contract execution environments and gas-efficient transaction processing

improve cryptographic methods to protect sensitive data. These directions aim to improve blockchain access control technology for modern cloud environments.

Acknowledgements
The authors extend their appreciation to Taif University, Saudi Arabia, for supporting this work through project number (TU-DSPP-2024-68).

Author contributions
All authors reviewed the manuscript. Idea and concept generation: Aarti Punia; Methodology: Preeti Gulia, Implementation: Nasib Singh Gill, Literature Review, Ebuka Ibeke, Supervision: Celestine Iwendi, Review Manuscript Draft: Piyush Kumar Shukla.

Data availability
N funding is available for this research work.

Declarations

Ethics approval and consent to participate
Not applicable.

Conflict of interest
The authors declare no conflicts of interest to report regarding the present study.

Received: 30 April 2024 / Accepted: 10 August 2024
Published online: 30 September 2024

References

1. Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N (Jan. 2023) Cloud Security threats and solutions: a Survey. Wirel Pers Commun 128(1):387–413. https://doi.org/10.1007/s11277-022-09960-z
2. Rani S, Bhambri P, Kataria A, Khang A, Sivaraman AK (2023) Big Data, Cloud Computing and IoT: tools and applications. CRC
3. Chinnasamy P, Deepalakshmi P (Feb. 2022) HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. J Ambient Intell Hum Comput 13(2):1001–1019. https://doi.org/10.1007/s12652-021-02942-2
4. Kunduru AR (May 2023) Security Concerns and Solutions for Enterprise Cloud Computing Applications. AJRCoS 15(4):24–33. https://doi.org/10.9734/ajrcos/2023/v15i4327
5. Chinnasamy P, Deepalakshmi P (2018) A scalable multilabel-based access control as a service for the cloud (SMBACaaS). Trans Emerg Telecommunications Technol 29(8):e3458. https://doi.org/10.1002/ett.3458

6. Vegesna VV A Critical Investigation and Analysis of Strategic Techniques Before Approving Cloud Computing Service Frameworks. Rochester, NY, Oct. 25, 2023. Accessed: Apr. 29, 2024. [Online]. Available: https://papers.ssrn.com/abstract=4612531
7. Overview of the Snowflake Breach Threat Actor Offers Data of Cloud Company's Customers, SOCRadar® Cyber Intelligence Inc. Accessed: Jun. 06, 2024. [Online]. Available: https://socradar.io/overview-of-the-snowflake-breach/
8. Trello data scraping Atlassian Community. Accessed: Jun. 06, 2024. [Online]. Available: https://community.atlassian.com/t5/Trello-discussions/Trello-data-scraping/td-p/2587475
9. Bank of America Informs Customers About 90-Day-Old Cyber Attack – Forbes Advisor. Accessed: Jun. 06, 2024. [Online]. Available: https://www.forbes.com/advisor/personal-finance/data-breach-affects-bank-of-america-customers/
10. Li W, Wu J, Cao J, Chen N, Zhang Q, Buyya R (Jun. 2021) Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. J Cloud Comput 10(1):35. https://doi.org/10.1186/s13677-021-00247-5
11. Gajmal Y, More P, Jagtap A, Kale K (Jan. 2024) Access control and data sharing mechanism in decentralized cloud using blockchain technology. J Autonom Intell 7(3). https://doi.org/10.32629/jai.v7i3.1332
12. Sharma P, Jindal R, Borah MD (Feb. 2023) A review of smart contract-based platforms, applications, and challenges. Cluster Comput 26(1):395–421. https://doi.org/10.1007/s10586-021-03491-1
13. Yang L et al (2024) Feb., An access control model based on blockchain master-sidechain collaboration, *Cluster Comput*, vol. 27, no. 1, pp. 477–497, https://doi.org/10.1007/s10586-022-03964-x
14. Chinnasamy P, Albakri A, Khan M, Raja AA, Kiran A, Babu JC (Jan. 2023) Appl Sci 13 6, Art. 6. https://doi.org/10.3390/app13063970Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System
15. Li D, Han D, Crespi N, Minerva R, Li K-C (Jan. 2023) A blockchain-based secure storage and access control scheme for supply chain finance. J Supercomput 79(1):109–138. https://doi.org/10.1007/s11227-022-04655-5
16. Fang J, Feng T, Guo X, Ma R, Lu Y (Feb. 2024) Blockchain-Cloud privacy-enhanced distributed industrial data trading based on verifiable credentials. J Cloud Comp 13(1):30. https://doi.org/10.1186/s13677-023-00530-7
17. Routh AK, Ranjan P (2024) A Comprehensive Review on Granularity Perspective of the Access Control Models in Cloud Computing, in *IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Mar. 2024, pp. 1–6. https://doi.org/10.1109/IATMSI60426.2024.10503154
18. Patil P, Sangeetha M, Bhaskar V (Apr. 2021) Blockchain for IoT Access Control, Security and privacy: a review. Wirel Pers Commun 117(3):1815–1834. https://doi.org/10.1007/s11277-020-07947-2
19. Butun I, Österberg P (2021) A review of distributed Access Control for Blockchain Systems towards securing the internet of things. IEEE Access 9:5428–5441. https://doi.org/10.1109/ACCESS.2020.3047902
20. Wijesekara PADSN (2024) A Literature Review on Access Control in Networking Employing Blockchain, *ijcs*, vol. 13, no. 1, Feb. https://doi.org/10.33022/ijcs.v13i1.3764
21. Sharma P, Jindal R, Borah MD (2020) Blockchain Technology for Cloud Storage: A Systematic Literature Review, *ACM Comput. Surv*, vol. 53, no. 4, p. 89:1–89:32, Aug. https://doi.org/10.1145/3403954
22. Praharaj L, Gupta M (2023) A systematic review of Access Control in Cloud Computing. in Future Connected technologies. CRC
23. Liu T, Wu J, Li J, Li J, Li Y (2023) Efficient decentralized access control for secure data sharing in cloud computing. Concurrency Computation: Pract Experience 35(17):e6383. https://doi.org/10.1002/cpe.6383
24. Saxena UR, Alam T (2023) Provisioning trust-oriented role-based access control for maintaining data integrity in cloud, *Int J Syst Assur Eng Manag*, vol. 14, no. 6, pp. 2559–2578, Dec. https://doi.org/10.1007/s13198-023-02112-x
25. BenMarak O, Naanaa A, Elasmi S (2024) A security evaluation of Chaos Attribute-based Access Control (ABAC) for Cloud Computing. In: Barolli L (ed) Advanced Information networking and applications. Springer Nature Switzerland, Cham, pp 415–425. https://doi.org/10.1007/978-3-031-57870-0_37.
26. Nakamura S, Takizawa M (2024) Trust Zone Model with the Mandatory Access Control Model. In: Barolli L (ed) in Advances in internet, data & web technologies. Springer Nature Switzerland, Cham, pp 512–521. https://doi.org/10.1007/978-3-031-53555-0_49.
27. Jamil MN, Hossain MS, Islam RU, Andersson K (2023) Workload Orchestration in Multi-access Edge Computing using belief rule-based Approach. IEEE Access 11:118002–118023. https://doi.org/10.1109/ACCESS.2023.3326244
28. Kumar Pawan G, Mohan Hari P, Amit S, Sanyam A (2024) Improving security, privacy, and trust in Cloud Computing. IGI Global
29. de Oliveira MT, Verginadis Y, Reis LHA, Psarra E, Patiniotakis I, Olabarriaga SD (2023) AC-ABAC: Attribute-based access control for electronic medical records during acute care, *Expert Systems with Applications*, vol. 213, p. 119271, Mar. https://doi.org/10.1016/j.eswa.2022.119271
30. Zhuang Y, Sun Y, Deng H, Guo J (Jan. 2023) Research on big data access control mechanism. Int J Comput Sci Eng 26(2):192–198. https://doi.org/10.1504/IJCSE.2023.129738
31. Brimhall B, Garrard J, De La Garza C, Coffman J, May, A Comparative Analysis of Linux Mandatory Access Control Policy Enforcement Mechanisms (2023), in *Proceedings of the 16th European Workshop on System Security*, Rome Italy: ACM, pp. 1–7. https://doi.org/10.1145/3578357.3589454
32. Shan F, Li F, Ji P (2023) A smart access control mechanism based on user preference in online social networks. Concurrency Computation: Pract Experience 35(20):e6864. https://doi.org/10.1002/cpe.6864
33. Nakamoto S Bitcoin: A Peer-to-Peer Electronic Cash System
34. Li J, Kassem M (Dec. 2021) Applications of distributed ledger technology (DLT) and blockchain-enabled smart contracts in construction. Autom Constr 132:103955. https://doi.org/10.1016/j.autcon.2021.103955
35. Politou E, Alepis E, Virvou M, Patsakis C (2022) Privacy in Blockchain. In: Politou E, Alepis E, Virvou M, Patsakis C (eds) in Privacy and Data Protection challenges in the distributed era. Springer International Publishing, Cham, pp 133–149. https://doi.org/10.1007/978-3-030-85443-0_7.
36. Blockchain Technology Market Size &, Growth, Report (2030) Accessed: Apr. 29, 2024. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market
37. Petersen K, Vakkalanka S, Kuzniarz L (Aug. 2015) Guidelines for conducting systematic mapping studies in software engineering: an update. Inf Softw Technol 64:1–18. https://doi.org/10.1016/j.infsof.2015.03.007
38. Alzoubi YI, Gill A, Mishra A (Nov. 2022) A systematic review of the purposes of Blockchain and fog computing integration: classification and open issues. J Cloud Comput 11(1):80. https://doi.org/10.1186/s13677-022-00353-y
39. Putra GD, Dedeoglu V, Kanhere SS, Jurdak R (2020) Trust Management in Decentralized IoT Access Control System, in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2020, pp. 1–9. https://doi.org/10.1109/ICBC48266.2020.9169481
40. Ur Rahman M, Guidi B, Baiardi F (2020) Blockchain-based access control management for Decentralized Online Social Networks, *Journal of Parallel and Distributed Computing*, vol. 144, pp. 41–54, Oct. https://doi.org/10.1016/j.jpdc.2020.05.011
41. Putra GD, Dedeoglu V, Kanhere SS, Jurdak R, Ignjatovic A (2021) Trust-Based Blockchain Authorization for IoT, *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1646–1658, Jun. https://doi.org/10.1109/TNSM.2021.3077276
42. Rizal Batubara F, Ubacht J, Janssen M (2019) Unraveling Transparency and Accountability in Blockchain, in *Proceedings of the 20th Annual International Conference on Digital Government Research*, in dg.o 2019. New York, NY, USA: Association for Computing Machinery, Jun. pp. 204–213. https://doi.org/10.1145/3325112.3325262
43. Rouhani S, Belchior R, Cruz RS, Deters R (2021) Distributed attribute-based access control system using permissioned blockchain, *World Wide Web*, vol. 24, no. 5, pp. 1617–1644, Sep. https://doi.org/10.1007/s11280-021-00874-7
44. Sultana T, Almogren A, Akbar M, Zuair M, Ullah I, Javaid N (2020) Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices, *Applied Sciences*, vol. 10, no. 2, Art. no. 2, Jan. https://doi.org/10.3390/app10020488
45. Kamboj P, Khare S, Pal S (2021) User authentication using Blockchain based smart contract in role-based access control, *Peer-to-Peer Netw. Appl*, vol. 14, no. 5, pp. 2961–2976, Sep. https://doi.org/10.1007/s12083-021-01150-1
46. Aftab MU et al (2022) Traditional and Hybrid Access Control Models: A Detailed Survey, *Security and Communication Networks*, vol. p. e1560885, Feb. 2022, https://doi.org/10.1155/2022/1560885
47. Gitlan D SHA-256 Algorithm - A Non-Technical Guide, SSL Dragon. Accessed: Jun. 06, 2024. [Online]. Available: https://www.ssldragon.com/blog/sha-256-algorithm/
48. Dolmeta A, Martina M, Masera G (2023) Comparative Study of Keccak SHA-3 Implementations, *Cryptography*, vol. 7, no. 4, Art. no. 4, Dec. https://doi.org/10.3390/cryptography7040060
49. Guo J, Karpman P, Nikolić I, Wang L, Wu S (2014) Analysis of BLAKE2. In: Benaloh J (ed) Topics in cryptology – CT-RSA 2014. Springer International Publishing, Cham, pp 402–423. https://doi.org/10.1007/978-3-319-04852-9_21.

50. Lam DK, Le VTD, Tran TH (2022) Efficient Architectures for Full Hardware Scrypt-Based Block Hashing System, *Electronics*, vol. 11, no. 7, Art. no. 7, Jan. https://doi.org/10.3390/electronics11071068
51. Liu F et al (2023) Analysis of RIPEMD-160: new collision attacks and finding characteristics with MILP. In: Hazay C, Stam M (eds) in Advances in cryptology – EUROCRYPT 2023. Springer Nature Switzerland, Cham, pp 189–219. https://doi.org/10.1007/978-3-031-30634-1_7.
52. Hlobaz A, Statistical Analysis of Enhanced SDEx Encryption Method Based on SHA-512 Hash Function, in (2020) *29th International Conference on Computer Communications and* Networks *(ICCCN)*, Honolulu, HI, USA: IEEE, Aug. 2020, pp. 1–6. https://doi.org/10.1109/ICCCN49398.2020.9209663
53. Sadeghi-Nasab A, Rafe V (2023) A comprehensive review of the security flaws of hashing algorithms, *J Comput Virol Hack Tech*, vol. 19, no. 2, pp. 287–302, Jun. https://doi.org/10.1007/s11416-022-00447-w
54. Aggarwal S, Kumar N (2021) Hashes☆, in *Advances in Computers*, vol. 121, S. Aggarwal, N. Kumar, and P. Raj, Eds., in The Blockchain Technology for Secure and Smart Applications across Industry Verticals, vol. 121., Elsevier, pp. 83–93. https://doi.org/10.1016/bs.adcom.2020.08.003
55. Ethash, GitHub Accessed: Jun. 07, 2024. [Online]. Available: https://github.com/ethereum/wiki/wiki/Ethash
56. Kaur G, Singh K, Gill HS (2021) Chaos-based joint speech encryption scheme using SHA-1, *Multimed Tools Appl*, vol. 80, no. 7, pp. 10927–10947, Mar. https://doi.org/10.1007/s11042-020-10223-x
57. Makhtoum HEL, Bentaleb Y (2022) Comparative study of Keccak and Blake2 hash functions. In: Ben Ahmed M, Teodorescu H-NL, Mazri T, Subashini P, Boudhir AA (eds) in Networking, Intelligent systems and Security. Springer, Singapore, pp 343–350. https://doi.org/10.1007/978-981-16-3637-0_24.
58. Eum S, Kim H, Song M, Seo H (2023) Optimized Implementation of Argon2 Utilizing the Graphics Processing Unit, *Applied Sciences*, vol. 13, no. 16, Art. no. 16, Jan. https://doi.org/10.3390/app13169295
59. Gauravaram P et al (2008) Grøstl - a SHA-3 candidate. Sep
60. Al-Shareefi F, Al-Barmani Z (2024) Comparing two cryptographic hash algorithms: SHA-512 and whirlpool- a case study on file integrity monitoring. BIO Web Conf 97:00093. https://doi.org/10.1051/bioconf/20249700093
61. V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine et al., Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain, *IJCNIS*, vol. 13, no. 2, pp. 1–15, (2021) https://doi.org/10.5815/ijcnis.2021.02.01
62. Abed S, Jaffal R, Mohd BJ, Al-Shayeji M (2021) An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices, *Cluster Comput*, vol. 24, no. 4, pp. 3065–3084, Dec. https://doi.org/10.1007/s10586-021-03324-1
63. Ferdous MS, Chowdhury MJM, Hoque MA (May 2021) A survey of consensus algorithms in public blockchain systems for crypto-currencies. J Netw Comput Appl 182:103035. https://doi.org/10.1016/j.jnca.2021.103035
64. Tetu J-F, Trudeau L-C, Van Beirendonck M, Balatsoukas-Stimming A, Giard P (2020) A Standalone FPGA-Based Miner for Lyra2REv2 Cryptocurrencies, *IEEE Trans. Circuits Syst. I*, vol. 67, no. 4, pp. 1194–1206, Apr. https://doi.org/10.1109/TCSI.2020.2970923
65. Sandeepkumar EV, Suresh A, Blockchain Assisted Cloud Storage For Electronic Health Records, in (2023) *International Conference on Computer Communication and* Informatics *(ICCCI)*, Jan. 2023, pp. 1–6. https://doi.org/10.1109/ICCCI56745.2023.10128219
66. Kumar A, Abhishek K, Bhushan B, Chakraborty C (2021) RETRACTED ARTICLE: Secure access control for manufacturing sector with application of ethereum blockchain, *Peer-to-Peer Netw. Appl*, vol. 14, no. 5, pp. 3058–3074, Sep. https://doi.org/10.1007/s12083-021-01108-3
67. Jia C, Geng Y, Sun S, Research on Data Access Management Based on Blockchain Engine (2022), *International Conference on Big Data, Information and Computer* Network *(BDICN)*, Jan. 2022, pp. 465–468. https://doi.org/10.1109/BDICN55575.2022.00091
68. Zou Y, Peng T, Zhong W, Guan K, Wang G (2022) Reliable and Controllable Data Sharing Based on Blockchain, in *Ubiquitous Security*, G. Wang, K.-K. R. Choo, R. K. L. Ko, Y. Xu, and B. Crispo, Eds., Singapore: Springer, pp. 229–240. https://doi.org/10.1007/978-981-19-0468-4_17
69. Algarni S et al (2021) Jan., Blockchain-Based Secured Access Control in an IoT System, *Applied Sciences*, vol. 11, no. 4, Art. no. 4, https://doi.org/10.3390/app11041772
70. Boumezbeur I, Zarour K (Mar. 2022) Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology. Acta Informatica Pragensia 11:105–122. https://doi.org/10.18267/j.aip.176
71. Chen Z, Xu W, Wang B, Yu H (Nov. 2021) A blockchain-based preserving and sharing system for medical data privacy. Future Generation Comput Syst 124:338–350. https://doi.org/10.1016/j.future.2021.05.023
72. Yang W, Guan Z, Wu L, Du X, Guizani M (May 2021) An Edge Blockchain Approach. IEEE Internet Things J 8(10):8632–8643. https://doi.org/10.1109/JIOT.2020.3047640. Secure Data Access Control With Fair Accountability in Smart Grid Data Sharing:
73. Liu Y, Zhang J, Zhan J (2021) Privacy protection for fog computing and the internet of things data based on blockchain, *Cluster Comput*, vol. 24, no. 2, pp. 1331–1345, Jun. https://doi.org/10.1007/s10586-020-03190-3
74. Fan Y et al (2019) Oct., TraceChain: A blockchain-based scheme to protect data confidentiality and traceability, *Software: Practice and Experience*, vol. 52, https://doi.org/10.1002/spe.2753
75. Gowda NC, Manvi SS, B. M. A., and, Lorenz P (May 2023) BSKM-FC: Blockchain-based secured key management in a fog computing environment. Future Generation Comput Syst 142:276–291. https://doi.org/10.1016/j.future.2022.12.042
76. Na D, Park S (2022) Blockchain-based Dashcam Video Management Method for data sharing and Integrity in V2V Network. IEEE Access 10:3307–3319. https://doi.org/10.1109/ACCESS.2022.3140419
77. Praveena Anjelin D, Ganesh Kumar S (2021) Blockchain Technology for Data sharing in decentralized Storage System. In: Dash SS, Das S, Panigrahi BK (eds) in Intelligent Computing and Applications. Springer, Singapore, pp 369–382. https://doi.org/10.1007/978-981-15-5566-4_32.
78. Huang H, Sun X, Xiao F, Zhu P, Wang W (Feb. 2021) Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. J Parallel Distrib Comput 148:46–57. https://doi.org/10.1016/j.jpdc.2020.10.002
79. Li X, Blockchain-Based A (2022) Verifiable User Data Access Control Policy for Secured Cloud Data Storage, *Computational Intelligence and Neuroscience*, vol. p. e2254411, Apr. 2022, https://doi.org/10.1155/2022/2254411
80. Deng H, Meng X, Guo J, Xi E, Zhao H (2020) A Framework of Blockchain-Based Security for WBANs, in *3rd International Conference on Smart BlockChain (SmartBlock)*, Oct. 2020, pp. 75–80. https://doi.org/10.1109/SmartBlock52591.2020.00021
81. Prasad PS, Beena Bethel GN, Singh N, Kumar Gunjan V, Basir S, Miah S (2022) [Retracted] Blockchain-Based Privacy Access Control Mechanism and Collaborative Analysis for Medical Images, *Security and Communication Networks*, vol. p. e9579611, Jun. 2022, https://doi.org/10.1155/2022/9579611
82. Hoang V-H, Lehtihet E, Ghamri-Doudane Y (2020) Privacy-preserving blockchain-based data sharing platform for decentralized Storage systems. Jun
83. Zhou W, Jin J, Blockchain-Based A Access Control Framework for Secured Data Sharing in Industrial Internet, in (2020) *Eighth International Conference on Advanced Cloud and Big* Data *(CBD)*, Dec. 2020, pp. 231–236. https://doi.org/10.1109/CBD51900.2020.00049
84. Spoorti H, Sneha R, Soujanya V, Heena K, Pooja S, Narayan DG (2021) Secure Access Control to Cloud Resources using Blockchain, in *IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, Nov. 2021, pp. 164–169. https://doi.org/10.1109/DISCOVER52564.2021.9663647
85. Kumar S, Singhal A, Dumka A (2019) Analysis of Cloud Security Framework using Blockchain Technology. Rochester, NY. 05. https://doi.org/10.2139/ssrn.3383151
86. Wang S, Zhang Y, Zhang Y (2018) A blockchain-based Framework for Data sharing with fine-Grained Access Control in Decentralized Storage systems. IEEE Access 6:38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611
87. Gao H, Luo S, Ma Z, Yan X, Xu Y (2021) 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. p. e5340116, Nov. 2021, https://doi.org/10.1155/2021/5340116
88. Zhang Y, Xiong L, Li F, Niu X, Wu H (Sep. 2023) A blockchain-based privacy-preserving auditable authentication scheme with hierarchical access control for mobile cloud computing. J Syst Architect 142:102949. https://doi.org/10.1016/j.sysarc.2023.102949
89. Ch R (2022) Design a decentralized secure access control network using blockchain on a cloud platform. Rev Preprint Sep. https://doi.org/10.21203/rs.3.rs-2031082/v1
90. Le T, Mutka MW (2018) CapChain: A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments, in *IEEE International Conference on Smart Computing (SMARTCOMP)*, Taormina: IEEE, Jun. 2018, pp. 57–64. https://doi.org/10.1109/SMARTCOMP.2018.00074

91. Wang H, Song Y (2018) Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain, *J Med Syst*, vol. 42, no. 8, p. 152, Aug. https://doi.org/10.1007/s10916-018-0994-6
92. Yan L, Ge L, Wang Z, Zhang G, Xu J, Hu Z (Apr. 2023) Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. J Cloud Comput 12(1):61. https://doi.org/10.1186/s13677-023-00444-4
93. Tan L, Shi N, Yu K, Aloqaily M, Jararweh Y (2021) A Blockchain-empowered Access Control Framework for Smart Devices in Green Internet of Things, *ACM Trans. Internet Technol*, vol. 21, no. 3, p. 80:1–80:20, Jun. https://doi.org/10.1145/3433542
94. Truong H et al (2022) [Retracted] Enabling Decentralized and Auditable Access Control for IoT through Blockchain and Smart Contracts, *Security and Communication Networks*, vol. p. e1828747, Jun. 2022, https://doi.org/10.1155/2022/1828747
95. Deebak BD, AL-Turjman F (Jan. 2022) A robust and distributed architecture for 5G-enabled networks in the smart blockchain era. Comput Commun 181:293–308. https://doi.org/10.1016/j.comcom.2021.10.015
96. Marwan M, Temghart AA, Sifou F, AlShahwan F (2020) A decentralized blockchain-based Architecture for a Secure Cloud-enabled IoT. JMM Nov. https://doi.org/10.13052/jmm1550-4646.1636
97. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2021) A Cooperative Architecture of Data Offloading and Sharing for Smart Healthcare with Blockchain, in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2021, pp. 1–8. https://doi.org/10.1109/ICBC51069.2021.9461063
98. Tariq F, Khan Z, Sultana T, Rehman M, Shahzad Q, Javaid N (2020) *Leveraging Fine-grained Access Control in Blockchain-based Healthcare System*
99. Malamas V, Kotzanikolaou P, Dasaklis TK, Burmester M (2020) A hierarchical Multi Blockchain for Fine Grained Access to Medical Data. IEEE Access 8:134393–134412. https://doi.org/10.1109/ACCESS.2020.3011201
100. Wang S, Wang X, Zhang Y (2019) A Secure Cloud Storage Framework with Access Control based on Blockchain. IEEE Access 7:112713–112725. https://doi.org/10.1109/ACCESS.2019.2929205
101. Singhal J, Gautam AS, Bhatia A, Agrawal A, Kaushik R (2022) DD-Locker: Blockchain-based Decentralized Personal Document Locker, in *International Conference on Information Networking (ICOIN)*, Jan. 2022, pp. 68–73. https://doi.org/10.1109/ICOIN53446.2022.9687236
102. Sharma P, Jindal R, Borah MD (Nov. 2021) Blockchain-based decentralized architecture for cloud storage system. J Inform Secur Appl 62:102970. https://doi.org/10.1016/j.jisa.2021.102970
103. Tharani JS, Tharmakulasingam M, Muthukkumarasamy V (Jan. 2020) A blockchain-based database management system. Knowl Eng Rev 35:e. https://doi.org/10.1017/S0269888920000302
104. Haritha T, Anitha A (2023) Multi-level Security in Healthcare by integrating lattice-based Access Control and Blockchain- based smart contracts system. IEEE Access 11:114322–114340. https://doi.org/10.1109/ACCESS.2023.3324740
105. Xiao M, Huang Q, Miao Y, Li S, Susilo W (2022) Blockchain Based Multi-Authority Fine-Grained Access Control System With Flexible Revocation, *IEEE Transactions on Services Computing*, vol. 15, no. 6, pp. 3143–3155, Nov. https://doi.org/10.1109/TSC.2021.3086023
106. Sharma S, Sharma P, Secure Software Updates for Resource-Constrained IoT on The Blockchain, in (2023) *3rd International Conference on Advance Computing and Innovative* Technologies *in Engineering (ICACITE)*, May 2023, pp. 1612–1616. https://doi.org/10.1109/ICACITE57410.2023.10182546
107. Liu Y et al (2023) Secure and scalable Cross-domain Data sharing in zero-Trust Cloud-Edge-End Environment based on Sharding Blockchain. IEEE Trans Dependable Secur Comput 1–14. https://doi.org/10.1109/TDSC.2023.3313799
108. Rohini K, Kala R, Kavitha C, Hema R, Praveen Kumar P (2020) Industrial IoT with Light-Weighted supporting hierarchical storage in distributed co-operative network for Blockchain Technology. in The Convergence of Artificial Intelligence and Blockchain technologies. WORLD SCIENTIFIC, pp 201–220. https://doi.org/10.1142/9789811225079_0010.
109. Zhang J, Yang Y, Liu X, Ma J (2022) An Efficient Blockchain-Based Hierarchical Data Sharing for Healthcare Internet of Things, *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7139–7150, Oct. https://doi.org/10.1109/TII.2022.3145851
110. Sravanthi K et al (2024) An Efficient Multi-User Groupwise Integrity CP-ABE(GI-CPABE) for Homogeneous and Heterogeneous Cloud Blockchain Transactions, *Journal of Electrical Systems*, vol. 20, no. 1, Art. no. 1, Jan. https://doi.org/10.52783/jes.685
111. Showkat S, Qureshi S (2022) Integration of Big Data, Machine Learning, and Blockchain Technology, in *Machine Learning Adoption in Blockchain-Based Intelligent Manufacturing*. CRC
112. Sarfaraz A, Chakrabortty R, Essam D (2022) AccessChain: An Access Control Framework to Protect Data Access in Blockchain Enabled Supply Chain, Computer Science and Mathematics, preprint, Feb. https://doi.org/10.20944/preprints202202.0106.v1
113. Alamri B, Crowley K, Richardson I (2022) Blockchain-Based Identity Management Systems in Health IoT: a systematic review. IEEE Access 10:59612–59629. https://doi.org/10.1109/ACCESS.2022.3180367
114. Kawalkar SA, Bhoyar DB (2024) Design of an Efficient Cloud Security Model through Federated Learning, Blockchain, AI-Driven Policies, and Zero Trust Frameworks, *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 10s, Art. no. 10s, Jan
115. Omrčen L, Leventić H, Romić K, Galić I (2021) Integration of Blockchain and AI in EHR sharing: A survey, in *2021 International Symposium ELMAR*, Sep. pp. 155–160. https://doi.org/10.1109/ELMAR52657.2021.9550953
116. Jayasudha M, Vijayalakshmi C (2022) Blockchain meets healthcare: Architecture for secure data sharing in unobtrusive medical applications, *AIP Conference Proceedings*, vol. 2405, no. 1, p. 020025, Apr. https://doi.org/10.1063/5.0072467
117. Zukarnain Z, Muneer A, Atirah N, Almohammedi A (2022) Medi-Block Record Secure Data Sharing in Healthcare System: Issues, Solutions and Challenges, *Computer Systems Science and Engineering*, Nov. https://doi.org/10.32604/csse.2023.034448
118. Chougule H, Dhadiwal S, Lokhande M, Naikade R, Patil R (Jan. 2022) Digital Evidence Management System for Cybercrime Investigation using Proxy Re-encryption and Blockchain. Procedia Comput Sci 215:71–77. https://doi.org/10.1016/j.procs.2022.12.008
119. Singh I, Singh B (2023) Integration of Decentralized BlockChain with Cloud & IoT Based SCM, in *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, May pp. 887–892. https://doi.org/10.1109/InCACCT57535.2023.10141797
120. Qaisar ZH, Almotiri SH, Al Ghamdi MA, Nagra AA, Ali G (2021) A scalable and efficient Multi-agent Architecture for Malware Protection in Data sharing over Mobile Cloud. IEEE Access 9:76248–76259. https://doi.org/10.1109/ACCESS.2021.3067284
121. Sun H, Tan Y, Zhu L, Zhang Q, Ai S, Zheng J (2023) A blockchain-based access control protocol for secure resource sharing with mobile edge-cloud collaboration, *J Ambient Intell Human Comput*, vol. 14, no. 10, pp. 13661–13672, Oct. https://doi.org/10.1007/s12652-022-04020-7
122. Li M, Qin Y (2021) Scaling the Blockchain-based Access Control Framework for IoT via Sharding, in *ICC - IEEE International Conference on Communications*, Jun. 2021, pp. 1–6. https://doi.org/10.1109/ICC42927.2021.9500403
123. Yu K, Tan L, Aloqaily M, Yang H, Jararweh Y (2021) Blockchain-Enhanced Data Sharing With Traceable and Direct Revocation in IIoT, *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7669–7678, Nov. https://doi.org/10.1109/TII.2021.3049141
124. Garg D, Bhatia KK, Gupta S (2021) A Research Perspective on Security in Fog Computing through Blockchain Technology. In: Solanki A, Sharma SK, Tarar S, Tomar P, Sharma S, Nayyar A (eds) in Artificial Intelligence and Sustainable Computing for Smart City. Springer International Publishing, Cham, pp 91–104. https://doi.org/10.1007/978-3-030-82322-1_7.
125. Imamguluyev R, Hasanov A, Mikayilova R (2023) Enhancing Node Selection in Blockchain-Enabled Edge Internet of Things (IoT): A Fuzzy Logic Approach for Improved Performance, in *7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Oct. 2023, pp. 37–41. https://doi.org/10.1109/I-SMAC58438.2023.10290320
126. Mallick SR, Goswami V, Lenka RK, Sharma S, Barik RK, Performance evaluation of Queueing assisted IoMT-Fog-Blockchain framework for healthcare organizations, in (2022) *IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer* Engineering *(UPCON)*, Dec. 2022, pp. 1–6. https://doi.org/10.1109/UPCON56432.2022.9986439
127. Mallick SR, Goswami V, Lenka RK, Patra S, Kumar V, Barik RK, Performance evaluation of priority Queueing assisted IoST-Fog-Blockchain framework in Geospatial Cloud Environment, in (2023) *International Conference on Microwave, Optical, and Communication* Engineering *(ICMOCE)*, May 2023, pp. 1–4. https://doi.org/10.1109/ICMOCE57812.2023.10167317
128. Fu L et al (Nov. 2023) Blockchain-enabled device command operation security for Industrial Internet of things. Future Generation Comput Syst 148:280–297. https://doi.org/10.1016/j.future.2023.06.004

129. Gai K, Wang S, Zhao H, She Y, Zhang Z, Zhu L (2023) Blockchain-Based Multisignature Lock for UAC in Metaverse, *IEEE Transactions on Computational Social Systems*, vol. 10, no. 5, pp. 2201–2213, Oct. https://doi.org/10.1109/TCSS.2022.3226717
130. Alshehri S, Bamasaq O, Alghazzawi D, Jamjoom A (2023) Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment, *IEEE Internet Things J*, vol. 10, no. 5, pp. 4239–4256, Mar. https://doi.org/10.1109/JIOT.2022.3217087
131. Qiu Y, Sun B, Dang Q, Du C, Li N (2022) IJACSA 13(10). https://doi.org/10.14569/IJACSA.2022.0131004. Fine-grained Access Control Method for Blockchain Data Sharing based on Cloud Platform Big Data
132. Song L, Ju X, Zhu Z, Li M (2021) An access control model for the Internet of Things based on zero-knowledge token and blockchain, *J Wireless Com Network*, vol. no. 1, p. 105, Dec. 2021, https://doi.org/10.1186/s13638-021-01986-4
133. Kebande VR, Awaysheh FM, Ikuesan RA, Alawadi SA, Alshehri MD (Jan. 2021) Sensors 21 18, Art. 18. https://doi.org/10.3390/s21186018A Blockchain-Based Multi-Factor Authentication Model for a Cloud-Enabled Internet of Vehicles
134. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2021) Secure Computation Offloading in Blockchain Based IoT Networks With Deep Reinforcement Learning, *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 3192–3208, Oct. https://doi.org/10.1109/TNSE.2021.3106956
135. Riad K, Elhoseny M (2022) A Blockchain-Based Key-Revocation Access Control for Open Banking, *Wireless Communications and Mobile Computing*, vol. p. e3200891, Jan. 2022, https://doi.org/10.1155/2022/3200891
136. Sohrabi N, Yi X, Tari Z, Khalil I (2020) BACC: Blockchain-Based Access Control For Cloud Data, in *Proceedings of the Australasian Computer Science Week Multiconference*, in ACSW '20. New York, NY, USA: Association for Computing Machinery, Feb. pp. 1–10. https://doi.org/10.1145/3373017.3373027
137. Qin X, Huang Y, Yang Z, Li X (Jan. 2021) A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. J Syst Architect 112:101854. https://doi.org/10.1016/j.sysarc.2020.101854
138. Khatiwada P, Yang B (2022) An access control and authentication scheme for secure data sharing in the decentralized cloud storage system, in *5th Conference on Cloud and Internet of Things (CIoT)*, Mar. 2022, pp. 137–144. https://doi.org/10.1109/CIoT53061.2022.9766634
139. Yao Y, Chang X, Mišić J, Mišić VB (2020) Lightweight and Privacy-Preserving ID-as-a-Service Provisioning in Vehicular Cloud Computing, *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2185–2194, Feb. https://doi.org/10.1109/TVT.2019.2960831
140. Alharbi A (2023) Applying Access Control Enabled Blockchain (ACE-BC) Framework to Manage Data Security in the CIS System, *Sensors*, vol. 23, no. 6, Art. no. 6, Jan. https://doi.org/10.3390/s23063020
141. Mahamuni N, Pattewar G, Nikam H, Loka O, Patil R (2023) A Blockchain and Proxy Re-encryption Based Approach for IoT Data Security: A Review, in *Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems*, M. A. Al-Sharafi, M. Al-Emran, M. N. Al-Kabi, and K. Shaalan, Eds., Cham: Springer International Publishing, pp. 587–595. https://doi.org/10.1007/978-3-031-25274-7_51
142. Ravi CN, Dinesh Krishnan S, Kaliyaperumal M, Kumar S, Ram Prasad AVS, and S. Suma Christal Mary, Blockchain-based Privacy-Preserving System for Internet of Things (IoT), in (2023) *8th International Conference on Communication and Electronics* Systems *(ICCES)*, Jun. 2023, pp. 309–315. https://doi.org/10.1109/ICCES57224.2023.10192790
143. George M, Mary Chacko A (2022) MediTrans—Patient-centric interoperability through blockchain. Int J Network Manage 32(3):e2187. https://doi.org/10.1002/nem.2187
144. Li T, Wang H, He D, Yu J (Aug. 2022) Blockchain-based privacy-preserving and rewarding private data sharing for IoT. IEEE Internet Things J 9(16):15138–15149. https://doi.org/10.1109/JIOT.2022.3147925
145. Kang G, Kim Y-G (Oct. 2022) Secure Collaborative Platform for Health Care Research in an Open Environment: perspective on accountability in Access Control. J Med Internet Res 24(10):e37978. https://doi.org/10.2196/37978
146. Du R, Ma C, Li M (2023) Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains, *Tsinghua Science and Technology*, vol. 28, no. 1, pp. 13–26, Feb. https://doi.org/10.26599/TST.2021.9010070
147. Zhang L, Li X, Wu Q, Rezaeibagha F (2024) Blockchain-Aided Anonymous Traceable and Revocable Access Control Scheme With Dynamic Policy Updating for the Cloud IoT, *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 526–542, Jan. https://doi.org/10.1109/JIOT.2023.3287190
148. Yang C, Tan L, Shi N, Xu B, Cao Y, Yu K (2020) AuthPrivacyChain: a blockchain-based Access Control Framework with privacy protection in Cloud. IEEE Access 8:70604–70615. https://doi.org/10.1109/ACCESS.2020.2985762
149. Pandiaraj A, Nagaraj P, Kumar PB, Rasi P, Lakshmi MN, Bhavani, Reddy CHV, Blockchain Using Private Cloud for Secure EHRS Systems, in (2023) *3rd International Conference on Pervasive Computing and Social* Networking *(ICPCSN)*, Jun. 2023, pp. 873–878. https://doi.org/10.1109/ICPCSN58827.2023.00149
150. Verma P, Tiwari R, Hong W-C (2023) Secure authentication in IoT Based Healthcare Management Environment using Integrated Fog Computing enabled Blockchain System. In: Tiwari R, Koundal D, Upadhyay S (eds) Image Based Computing for Food and Health Analytics: requirements, challenges, solutions and practices: IBCFHA. Springer International Publishing, Cham, pp 137–146. https://doi.org/10.1007/978-3-031-22959-6_8.
151. Sharma P, Jindal R, Borah MD (Apr. 2022) Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. J Supercomput 78:7700–7728. https://doi.org/10.1007/s11227-021-04179-4
152. Li C et al (2022) Dec., Efficient Medical Big Data Management With Keyword-Searchable Encryption in Healthchain, *IEEE Systems Journal*, vol. 16, no. 4, pp. 5521–5532, https://doi.org/10.1109/JSYST.2022.3173538
153. Jayatunga E, Nag A, Jurcut AD (2022) Security Requirements for Vehicle-to-Everything (V2X) Communications Integrated with Blockchain, in *Fourth International Conference on Blockchain Computing and Applications (BCCA)*, Sep. 2022, pp. 208–213. https://doi.org/10.1109/BCCA55292.2022.9922372
154. Li M et al (2024) Blockchain-Based Searchable Encryption Access Control Mechanism for the Internet of Things, in *Proceedings of the 13th International Conference on Computer Engineering and Networks*, Y. Zhang, L. Qi, Q. Liu, G. Yin, and X. Liu, Eds., Singapore: Springer Nature, pp. 258–268. https://doi.org/10.1007/978-981-99-9247-8_26
155. Deebak BD, Hwang SO (May 2024) Healthcare Applications using Blockchain with a cloud-assisted decentralized privacy-preserving Framework. IEEE Trans Mob Comput 23(5):5897–5916. https://doi.org/10.1109/TMC.2023.3315510
156. Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2019) Blockchain for Secure EHRs sharing of Mobile Cloud based E-Health systems. IEEE Access 7:66792–66806. https://doi.org/10.1109/ACCESS.2019.2917555
157. Wang Y, Zhang A, Zhang P, Wang H (2019) Cloud-assisted EHR sharing with security and Privacy Preservation via Consortium Blockchain. IEEE Access 7:136704–136719. https://doi.org/10.1109/ACCESS.2019.2943153
158. Al Breiki H, Al Qassem L, Salah K, Habib Ur Rehman M, Sevtinovic D, Decentralized Access Control for IoT Data Using Blockchain and Trusted Oracles, in (2019) *IEEE International Conference on Industrial* Internet *(ICII)*, Orlando, FL, USA: IEEE, Nov. 2019, pp. 248–257. https://doi.org/10.1109/ICII.2019.00051
159. Pateritsas A, Petrakis EGM (2023) iBot: secure and Trusted Access to IoT Data with Blockchain. In: Barolli L (ed) in Advanced Information networking and applications. Springer International Publishing, Cham, pp 521–533. https://doi.org/10.1007/978-3-031-29056-5_45.
160. Bisht T, Dinesh D, Usha G, Gautam K (2023) Edge Devices and Blockchain Integration in IoT System: A Novel Design Approach, in *International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Jan. 2023, pp. 35–40. https://doi.org/10.1109/IDCIoT56793.2023.10053481
161. Yang L, Zou W, Wang J, Tang Z (May 2022) EdgeShare: a blockchain-based edge data-sharing framework for Industrial Internet of things. Neurocomputing 485:219–232. https://doi.org/10.1016/j.neucom.2021.01.147
162. Fugkeaw S, Wirz L, Hak L (2023) Secure and Lightweight Blockchain-Enabled Access Control for Fog-assisted IoT Cloud Based Electronic Medical records sharing. IEEE Access 11:62998–63012. https://doi.org/10.1109/ACCESS.2023.3288332
163. Ma M, Shi G, Li F (2019) Privacy-oriented blockchain-based distributed Key Management Architecture for Hierarchical Access Control in the IoT scenario. IEEE Access 7:34045–34059. https://doi.org/10.1109/ACCESS.2019.2904042
164. Li H, Han D, Tang M (2021) Logisticschain: A Blockchain-Based Secure Storage Scheme for Logistics Data, *Mobile Information Systems*, vol. p. e8840399, Feb. 2021, https://doi.org/10.1155/2021/8840399
165. Jayasri R, Jayakumar D, Joshila Roselin S, Ramkumar MO, Plan of Block-chain Enabled Confirmed Key Management Protocol for Internet of Medical Things Development, in (2022) *3rd International Conference on Electronics and Sustainable Communication* Systems *(ICESC)*, Aug. 2022, pp. 668–673. https://doi.org/10.1109/ICESC54411.2022.9885295
166. Zheng K et al (Oct. 2022) Blockchain technology for enterprise credit information sharing in supply chain finance. J Innov Knowl 7(4):100256. https://doi.org/10.1016/j.jik.2022.100256
167. Noh S, Firdaus M, Qian Z, Rhee K-H, Blockchain-Based A (2023) Data Integrity auditing protocol for Smart HACCP. In: Park JS, Yang LT, Pan Y, Park JH (eds) in

Advances in Computer Science and ubiquitous Computing. Springer Nature, Singapore, pp 423–429. https://doi.org/10.1007/978-981-99-1252-0_56.
168. Han R, Wang Y, Wan M, Yuan T, Sun G (2023) FIBPRO: Peer-to-peer data management and sharing cloud storage system based on blockchain, *Peer-to-Peer Netw. Appl*, vol. 16, no. 6, pp. 2850–2864, Nov. https://doi.org/10.1007/s12083-023-01570-1
169. Qureshi KN, Jeon G, Hassan MM, Hassan MR, Kaur K (2023) Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems, *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7435–7443, Jul. https://doi.org/10.1109/TITS.2022.3158320
170. Li H, Pei L, Liao D, Chen S, Zhang M, Xu D (2020) A fine-Grained Access Control Scheme for VANET Data based on Blockchain. IEEE Access 8:85190–85203. https://doi.org/10.1109/ACCESS.2020.2992203
171. Guo J, Yang W, Lam K-Y, Yi X (2019) Using blockchain to Control Access to Cloud Data. In: Guo F, Huang X, Yung M (eds) in Information Security and Cryptology. Lecture Notes in Computer Science. Springer International Publishing, Cham, pp 274–288. https://doi.org/10.1007/978-3-030-14234-6_15.
172. Ri O-C, Kim Y-J, Jong Y-J Blockchain-based RBAC Model with separation of duties constraint in Cloud Environment.
173. Almasian M, Shafieinejad A (2024) Secure cloud file sharing scheme using blockchain and attribute-based encryption. Comput Stand Interfaces 87:103745. https://doi.org/10.1016/j.csi.2023.103745
174. Saini A, Zhu Q, Singh N, Xiang Y, Gao L, Zhang Y (2021) A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System, *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914–5925, Apr. https://doi.org/10.1109/JIOT.2020.3032997
175. Naresh VS, Reddi S, Allavarpu VVLD (2021) Blockchain-based patient centric health care communication system. Int J Commun Syst 34(7):e4749. https://doi.org/10.1002/dac.4749
176. Ding Y, Sato H (2020) Bloccess: Towards Fine-Grained Access Control Using Blockchain in a Distributed Untrustworthy Environment, in *8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Aug. 2020, pp. 17–22. https://doi.org/10.1109/MobileCloud48802.2020.00011
177. Chen Y, Meng L, Zhou H, Xue G (2021) A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection, *Wireless Communications and Mobile Computing*, vol. p. e6685762, Jul. 2021, https://doi.org/10.1155/2021/6685762
178. Doshi D, Khara S (2021) Blockchain-Based Decentralized Cloud Storage, in *International Conference on Mobile Computing and Sustainable Informatics*, J. S. Raj, Ed., Cham: Springer International Publishing, pp. 563–569. https://doi.org/10.1007/978-3-030-49795-8_54
179. Jabarulla MY, Lee H-N (2021) Blockchain-Based Distributed Patient-Centric Image Management System, *Applied Sciences*, vol. 11, no. 1, Art. no. 1, Jan. https://doi.org/10.3390/app11010196
180. Khare S, Badholia A (Apr. 2023) BLA2C2: design of a Novel Blockchain-based Light-Weight Authentication & Access Control Layer for Cloud Deployments. IJRITCC 11(3):283–294. https://doi.org/10.17762/ijritcc.v11i3.6359
181. Gajmal YM, Udayakumar R (2021) Blockchain-Based Access Control and Data Sharing Mechanism in Cloud Decentralized Storage System, *Journal of Web Engineering*, pp. 1359–1388, Aug. https://doi.org/10.13052/jwe1540-9589.2054
182. Li G, Wu H, Wu J, Li Z (May 2024) Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain. J Cloud Comp 13(1):97. https://doi.org/10.1186/s13677-024-00652-6
183. Saari A, Vimpari J, Junnila S (Oct. 2022) Blockchain in real estate: recent developments and empirical applications. Land Use Policy 121:106334. https://doi.org/10.1016/j.landusepol.2022.106334
184. Javaid M, Haleem A, Singh RP, Suman R, Khan S (Jul. 2022) A review of Blockchain Technology applications for financial services. BenchCouncil Trans Benchmarks Stand Evaluations 2(3):100073. https://doi.org/10.1016/j.tbench.2022.100073
185. Deepak et al (2024) Exploring the potential of Blockchain Technology in an IoT-Enabled environment: a review. IEEE Access 12:31197–31227. https://doi.org/10.1109/ACCESS.2024.3366656
186. Akbar MA, Mahmood S, Siemon D (2022) Toward Effective and Efficient DevOps using Blockchain, in *Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering*, in EASE '22. New York, NY, USA: Association for Computing Machinery, Jun. pp. 421–427. https://doi.org/10.1145/3530019.3531344
187. Loukil F, Abed M, Boukadi K (2021) Blockchain adoption in education: a systematic literature review, *Educ Inf Technol*, vol. 26, no. 5, pp. 5779–5797, Sep. https://doi.org/10.1007/s10639-021-10481-8
188. Tan E, Mahula S, Crompvoets J (Jan. 2022) Blockchain governance in the public sector: a conceptual framework for public management. Government Inform Q 39(1):101625. https://doi.org/10.1016/j.giq.2021.101625

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.