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

*Review Article*

# Data Visibility in Enterprise Distributed Ledger Technologies: A Systematic Review of Access Control and Anonymity Mechanisms

**Afeefa Noorain** [a], **Khaleel Ahmad** [a *], **Laura Emilia Maria Ricci** [b]

[a] Department of Computer Science and Information Technology, Maulana Azad National Urdu University (A Central University), Hyderabad, India.
[b] Department of Computer Science, University of Pisa, Pisa, Italy.

Submitted: 10 April 2026
Revised: 1 July 2026
Accepted: 6 July 2026

*** Corresponding Author**:
khaleelahmad@manuu.edu.in

**Keywords:** Data visibility, Distributed ledger technology, Enterprise DLT, Blockchain, Policies, Transparency, Immutability.

**How to cite this paper:** A. Noorain, K. Ahmed, L. E. M. Ricci, " Data Visibility in Enterprise Distributed Ledger Technologies: A Systematic Review of Access Control and Anonymity Mechanisms," KJAR, vol. 11, no. 2, pp. 1-32, December 2026, doi: 10.24017/science.2026.2.1



**Abstract:** Data visibility is more vital and decisive than ever before in the current data-driven world of technology. There is a significant upsurge in businesses leveraging digital technology, which has led to a greater amount of data being available than ever before. Additionally, managing the visibility in compliance with the organization's rules and regulations is crucial. The implementation of efficient data visibility will not merely improve decision-making but also streamline business processes with enhanced security. Numerous technologies offer solutions to manage data visibility, and distributed ledger technology (DLT) is one of them. DLT facilitates the execution of different methodologies to strengthen the governance of data visibility in enterprise-grade applications. On the other hand, these DLTs raise concerns regarding data visibility in this decentralized network, as not every enterprise-grade application requires data transparency across all the nodes. In this paper, a detailed systematic review is conducted with a clear focus on two essential data visibility parameters, Access control and anonymity, for the period 2020-2025, following a standardized Preferred Reporting Items for Systematic Review and Meta-Analyses -based breakdown of the selection process. Three clear dimensions of in-depth analysis are presented in the study: first, investigating how DLT can maintain transparency and decentralization in enterprise-grade applications; second, ensuring secure data access management for effective data governance; and third, the approach for anonymization to ensure privacy and security. The key finding highlights the credence of hyperledger fabric, a permissioned DLT, compared to other DLTs and exponentially growing concerns related to data visibility, as well as the conceptual and empirical research contributions made thus far. The limitations presented in this paper formulate a strong basis for research and enhancement of the existing models to offer controlled yet transparent data visibility.

## 1. Introduction

The term data visibility gained a lot of exposure in the early 2000s, and according to Jeong *et al.* [1], data visibility ensures that the data is accessible only to authorized users of distinct organizational hierarchy levels. It follows a punctilious and discriminative approach subject to user requirements and data specialization. For any organization, controlling this data visibility is crucial, as cross-functional data sharing should be done. In the preliminary phase of enabling data visibility, data was fragmented with minimal computation on relational tables, resulting in reasonable privacy-preserving access and confidentiality. Subsequently, by leveraging visibility constraints that define data privacy policies, adherence to these policies ensured legitimate access and maintained the confidentiality of sensitive information [2].

Establishing data visibility strategies and methods has far-reaching implications for diverse businesses. In supply chain management, data visibility is pivotal in decision-making and mitigating the risks involved in procurement, manufacturing, and delivery [3]. The availability of the required information of the supplier will enable informed decision-making by the manufacturers and minimize risk with increased cost efficiency [4]. Meanwhile, distributed ledger technology (DLT) has become a revolutionary approach across various industries and businesses as it guarantees transparency, immutability, and security, leading to well-informed decision-making. As stated in previous studies [5-8], supply chain transparency is essential to provide security and build trust among stakeholders through effective transparency policies, and blockchain, as a DLT, extends these capabilities. These policies are defined with appropriate disclosure agreements that function at different organizational levels to enhance the functional processes for quality assurance and potential evaluation.

DLT can boost the supply chain management system's transparency, traceability, and accuracy. On the contrary, data sparsity, classified as noise, bias, and missing values, is also an aspect that should be addressed to reinforce data visibility, as it influences the decision-making process and hinders data accessibility [9]. Additionally, several studies highlighted various facets of transparency that remain unexplored, while data visibility has been a constant concern [5-9].

It is apparent that data visibility is indispensable across all application domains, especially the healthcare industry, as all medical records are now being digitized. Well-defined fine-grained policies should be formally deployed to ensure the privacy of patients' electronic health records. These deployments are expected to offer an efficient privacy-preserving solution. Henceforth, several solutions based on big data, blockchain, internet of things (IoT), and artificial intelligence have been proposed by researchers to address security and privacy concerns [10-13]. With the increase in digitization and enterprise-grade applications, the demand for constrained and determined mechanisms of supervised data visibility is of utmost importance. This supervision can be done with a well-organized access control mechanism that can authorize, authenticate, and register every transaction on the data.

Data is a valuable resource on the internet that must be secured and guarded from unauthorized access and attacks. Several surveys were conducted to present the attacks, and their mitigation tools were developed [14, 15]. The privacy and security of data are always at stake because of security breaches and gaps, and the research continues to understand the attacks and countermeasures to control them using artificial intelligence, machine learning, and deep learning [16-20]. For most public, private, and government organizations, data continues to be stored and managed using traditional database management systems on the internet or a local server. Conventional database approaches used to protect data are insufficient because they rely on a centralized model for managing it. Various risks and vulnerabilities include distributed denial of service, malware, misconfigurations, and centralized maintenance. This centralization is the biggest drawback of this system [21].

To overcome the drawbacks of traditional databases and to provide a comprehensive solution that encompasses transparency, security, and cryptography, DLT was introduced, which is a decentralized system of nodes participating in a distributed network to manage structured and unstructured data [22].

In DLT, every node maintains its own copy of the ledger, and everything is transparent to all the peers in the network. This completely transparent DLT is called a public DLT. The problem with public DLTs is the data visibility to all the participants in the network. Hence, there are private and permissioned DLTs to handle privacy and confidentiality concerns. Private DLTs are generally created and maintained by a single organization and can be used for private data sharing within the organization. In permissioned DLTs, the ledger is visible to all the peers of participating authorized organizations, but not every peer will have complete access to the data. Hyperledger fabric is a permissioned distributed ledger that facilitates the development of enterprise-grade blockchain networks [23].

Various surveys have been published with a broader focus on privacy-preserving techniques in access control, such as blockchain, machine learning, and cryptography, utilized across various application domains [24], and others have narrowed it down [25] to either application or technique or both [26].

Some surveys focused on privacy and security threats as a comprehensive survey on various application domains [15, 16, 19]. Another set of surveys focused on security and privacy threats on blockchain [27], ethereum [28], smart contracts [29], all application domains with focus on security, privacy, and threat models [30]. The studies on zero-knowledge proof [31] as a technology and protocols [32] available added another focused dimension on identity management [33].

The contribution of this research is based on the following significant gaps:

- The techniques discussed in previous studies have several intricacies related to each one of them for privacy preservation that are under-researched.
- Lack of in-depth analysis on data visibility concerns in various DLTs. Scrutinizes security mitigation tools and protocols for the cloud environment or in a generic sense.
- Inadequate unified approach for integrating privacy and access control simultaneously.
- Anonymization is not treated as a privacy-preserving primitive in data visibility, but rather it is considered in isolation.
- Various challenges of DLTs are presented together, which disseminates research in multiple directions.

This paper presents a unified systematic survey with a spotlight on the key parameters of data visibility, access control, and anonymity in DLT. Additionally, it evaluates the types of DLT to identify the one that best suits enterprises. Furthermore, it expounds on the access control mechanisms within the DLT for managing data visibility and offers an insightful perspective on the current state of the research landscape.

The remainder of this paper is structured as follows. Section 2 highlights the research question (RQ)s and discusses the research methodology and strategy applied to gather the appropriate sources for the systematic literature review. Section 3 presents the outcome of the review focusing on enterprise-grade applications, DLT, access control mechanisms, and anonymity. Section 4 provides an in-depth discussion of the review. Finally, Section 5 concludes with challenges and proposed solutions.

## 2. Materials and Methods

This paper gives a clear perspective of different DLTs and their existing access control policies for the various application resources. This work also covers the other access control policies proposed and designed, as well as their drawbacks and benefits; it follows a systematic literature review style, beginning with the formulation of clear and concise RQs, which leads to the identification of the key aspects of this review. This is followed by understanding and appraising the research studies in the field of DLT, concentrating on data visibility.

### *2.1. Research Questions*

The paper is organized into distinct sections, each addressing the specific RQs. Subsections 3.1-3.5: in this section, the focus is on the intricate details of the review and gaining an understanding of an enterprise-grade application. The key features of enterprise-grade applications are considered to identify the technology required to support these features. This section gives a background of the technological evolution and answers the following RQs:

RQ 1.1: How does DLT support enterprise-grade applications?

Subsection 3.6: After identifying the technology, the concentration is shifted to the next important detail, which is to understand the main theme of this paper, data visibility. The components of DLT are described in this block to handle the problem related to data visibility. This section highlights the mechanisms available to provide data visibility with attention to the following RQs:

RQ 2.1: What is an access control mechanism, and how does it support data visibility?

RQ 2.2: What are the different access control mechanisms?

Subsection 3.7: Anonymity is a crucial aspect of this research because it extends the services of access control mechanisms discussed in the previous section by offering unlinkability and confidentiality. This section presents the importance of anonymity in enterprise-grade applications and aims to address the following RQs:

RQ 3.1: What is Anonymity and its significance?

RQ 3.2: What tools and libraries are used in hyperledger fabric to ensure anonymity?

Sections 4 & 5: Recognizing the significance of data visibility and anonymity, this section sheds light on the models and frameworks proposed for optimized performance. This section highlights the challenges faced by the researchers in their implementation, and the proposed future work and the following RQs are addressed:

RQ 4.1: What are the drawbacks of the proposed models, architecture, and frameworks?

RQ 4.2: What are the current tools and methods deployed to guarantee data visibility and anonymity?

### *2.2. Data Sources and Search Strategy*

This paper is written based on the search results of the research databases and their search engines: (1) Association for Computing Machinery (ACM) Digital Library, (2) ScienceDirect, (3) Institute of Electrical and Electronics Engineers (IEEE) Xplore, and (4) Springer Nature Link. The papers were shortlisted based on the search string formulated using the keywords related to the Research Questions as presented below:

(distributed ledger technology | DLT | public DLT | permissioned DLT | private DLT | enterprise DLT | Hyperledger Fabric) & (enterprise-grade application) & (data visibility) & (access control mechanism | access control list | ACM | privacy | secure access) & (anonymity | ZKP | identity management).

### *2.3. Inclusion and Exclusion Criteria*

The papers included followed these three inclusion criteria: address at least one of the relevant keywords of the RQs, published after 2020 and are in English and the papers with a valid proposal, implementation, and evaluation model or framework. The exclusion criteria followed for this study cover generic studies that deviate from the focus of this research, full-text not accessible and lacks implementation and validation, or the theoretical framework lacked sufficient implementation support. The preferred reporting items for systematic review and meta-analyses (PRISMA) flow diagram in figure 1 depicts the selection strategy of this paper, with the number of research articles or studies [34].

Potential sources of bias are identified to the extent possible in this paper. Grey literature was excluded, with a few exceptions to official documentation on DLT and hyperledger fabric. The selection of papers was made with multiple combinations of the search string defined, supplemented with forward and backward snowball searching. The inclusion and exclusion criteria defined and applied confirm that all papers have been critically analyzed and included without bias towards the identified gaps. A few foundational papers pre-2020 were considered despite the search window 2020-2025. The language bias is acknowledged as a limitation, as English is the predominant language.

## 3. Results

### *3.1. Enterprise-grade Application*

After the mid-20th Century, with the introduction of the operating system, application servers, and the supported programming languages, automating the processes to reduce human intervention was on the rise. During the industrial revolution 3.0 businesses were encouraged to automate their processes and streamline their workflows using the enterprise applications or software designed for record-keeping and processing the data stored [35]. This computerized automation marks the inception of the enterprise-grade application, a software application designed for large organizations from different sectors, ranging from supply chain management, enterprise resource planning, human resource management, customer relationship management, accounting, healthcare, and data management [36-41].

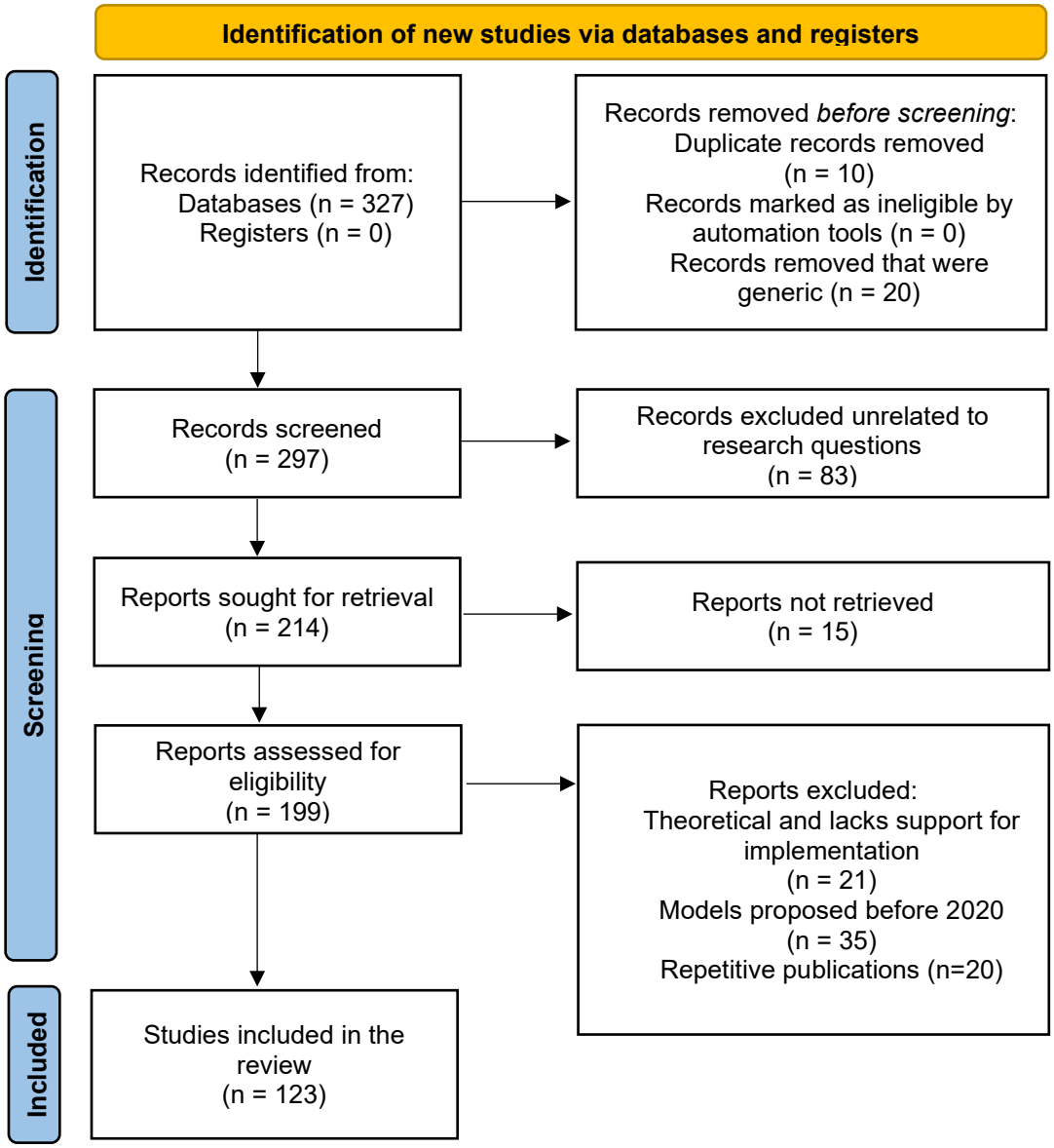


**Figure 1:** PRISMA flow diagram illustrating the identification, screening, eligibility, and inclusion of studies for the systematic review.

These enterprise-grade applications are designed for efficiency, reliability, productivity, and scalability to improve the overall performance of the operations and their workflows involved in managing a large-scale organization. These applications are also expected to provide a platform where multiple organizations of different sizes connect to contribute to decision-making and manage the workflows [4]. The application is expected to perform each of the activities of the workflow very smartly to increase the productivity of the business involved reduce operational costs and financial risks in order to generate better revenue [27].

The applications are designed in compliance with the organization's policies to ensure secure access and eliminate human intervention for performing repetitive tasks of verifying every single access request. Several technological advancements took place to fortify the expected security of the enterprise-grade application [41].

Subsection 3.2 describes distributed ledger technology, which focuses on enhancing efficiency, reliability, productivity, and scalability in enterprise-grade applications.

### *3.2. Distributed Ledger Technology*

In the early stages of introduction, enterprise-grade applications were designed with centralized data management. These applications were efficient and effectively advocated for the concept of automation during that era. However, the major drawbacks that were identified were a) single point of failure, b) centralized data storage governed by a single entity [42]. To overcome these major drawbacks, the concept of decentralization emerged, and many development companies began exploring the potential technologies that could support decentralization while guaranteeing the privacy, security, and integrity of data.

DLT has apparently become a viable solution to address concerns related to centralization. DLT is a peer-to-peer network of entities interested in collaborating to perform various business processes in an enterprise-grade application [43]. The term "ledger" in DLT signifies the record or log of transactions performed on the data, assuring transparency and eliminating the threat of a single point of failure. These ledgers are distributed across the network and get synchronized regularly to assert consistency, immutability, and decentralization [44]. As these ledgers are transparent and tamper-resistant, modifying the data with authorized or unauthorized privileges is highly unlikely. Each transaction request is endorsed by the initiator and is validated before it is committed to a block of the Blockchain and later appended to the ledger [45].

There are different types of DLTs with distinct features, and they can be adopted based on the implementation use case: a) public, b) private, and c) permissioned [46]. Figure 2 highlights the key differences among the three DLTs. The much-publicized examples of public DLT are Bitcoin [47] and Ethereum [28, 48]. On the basis of these use cases, the public DLT can be considered a permissionless network, open for everyone to participate without authorization and perform mining or commit a transaction according to the consensus mechanism followed by the network. Ethereum supported the implementation of many enterprise-grade applications managed by multiple organizations, like decentralized finance [49], decentralized autonomous organization [50], and non-fungible token [51].

In contrast, the private DLT network is more secure and has restricted access. It is designed to be managed by a single organization, and authorization is required to join this network [52]. Private DLT networks ensure privacy in terms of data propagation within the network, making them suitable for enterprise-grade applications. These DLTs enable individuals or organizations to manage their assets efficiently. Decentralized online social network was developed on an Ethereum permissioned network, leveraging smart contracts and interplanetary file system (IPFS) [53]. Initially, the smart contracts were written in the Solidity language, and in recent years, with the availability of Geth Go-ethereum [54], they can be written in the Go language with completely private nodes.

Every transaction in Ethereum incurs a transaction fee, which is basically the computational power required, measured as gas. The higher the gas price, the higher the chances that the miners will select the transaction for mining and commit to the block. The miners, in return, get rewarded according to the units of gas they have used in mining. As multiple nodes in the network will compete for this reward, reaching consensus is essential. Ethereum employs proof of work, proof of stake, and proof of authority. Ethereum transitioned from proof of work to proof of stake in 2022 to enhance sustainability by reducing power consumption. In DLT, for private networks, proof of authority is more appropriate, as it prioritizes the nodes as validators and miners, unlike the other two algorithms, where the computational power or the equity of nodes is considered [55]. In the case of private transactions, the major concern is the fee optimization problem, as these transactions are more complex and, at the same time, gas-intensive [29].


**Figure 2:** Mind map for types of DLT.

Unlike the public DLT, the permissioned DLT network is partially controlled, with a restricted number of nodes participating in the network [56]. Private and permissioned DLTs are both partially controlled, but are to some extent different in features like the number of organization(s) governing the network, privileged access grants, and in permissioned DLT, control can be shared with nodes of different organizations participating in the network. In short, it offers hybrid governance with selective access rights that can be granted to each node based on its role and other attributes [57]. These features guarantee transparency for enterprise-grade applications with decentralization [37].

An enterprise-grade application should ensure secure access to information by authorized users only, thereby attesting to the privacy of the information, making it more reliable [58]. Enterprise-grade applications deal with data that needs to be handled with utmost care, unlike cryptocurrency, where decentralization and transparency are essential and beneficial. These requirements can be capably met with permissioned blockchain, a type of permissioned DLT, as it offers transparency, security, privacy, and immutability, making it a more suitable choice for developing enterprise-grade applications [59]

[60]. A permissioned blockchain for these applications addresses the major concern of all the organizations where data is managed by either a centralized authority or a single organization, which puts the data at risk at any time in case of any natural calamity or illegitimate access by any user [61]. In a permissioned blockchain, every transaction can be tracked as it is cryptographically signed by the initiator and committed on the ledger and to the blockchain [62]. This asserts that permissioned blockchain technology offers constructive support for organizations to manage their workflows within and among the organizations.

To collaborate with multiple organizations, DLT extends its capability with the concept of a consortium blockchain [63]. An enterprise-grade application is typically designed to work with multiple organizations, where every pair or group of organizations works together for a specific workflow [64]. This alliance can be coherently strengthened and streamlined with the help of a consortium blockchain. In a consortium blockchain, the organizations can connect via a channel and communicate the information privately among the intended participating organizations [65].

The research databases, namely ACM Digital Library, IEEE Xplore, ScienceDirect, and Springer Nature Link, are searched for the keywords "public", "private", and "permissioned blockchain" to analyze the number of research articles published and surveys conducted. The results in figure 3 show that research activities for permissioned blockchain are notably low for the years 2023, 2024, and 2025.

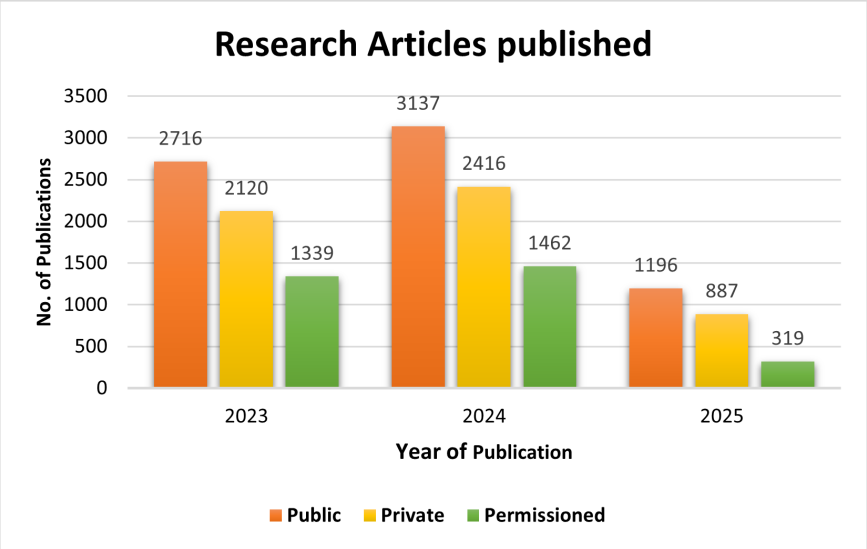


**Figure 3:** Comparative year-wise trend of published research articles (2023-2025).

The investigation into the same set of keywords led to the conclusion that the number of surveys and review articles for permissioned blockchain is comparatively lower than for public and permissioned blockchain, as illustrated in figure 4. The live count of publications may vary because of continuous indexing by these databases.

The insights gained from the above analysis emphasize the need to research and implement permissioned DLT for enterprises. Permissioned DLTs offer far more benefits compared to public and private blockchains, but they are still in their infancy and are gradually moving towards widespread adoption. This paper presents strong indications to advocate for the acceptance of permissioned DLT, especially for enterprise-grade applications. The requirements of enterprise-grade applications and the unique features of permissioned DLT complement each other very well to support the smooth operation of workflows within and between organizations. Building on the complementarity, the term Enterprise DLT can be established. The following subsection discusses this Enterprise DLT concept as it is inherited from Permissioned DLT.

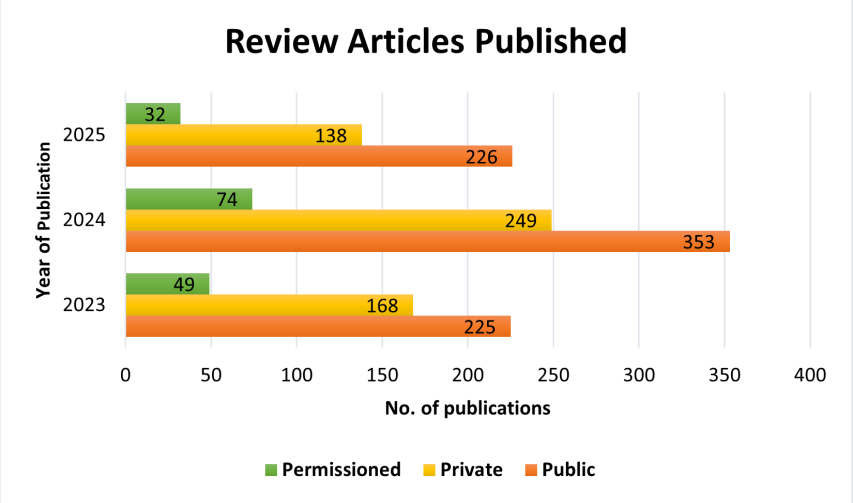


**Figure 4:** Comparative year-wise trend of published review articles (2023-2025).

### *3.3. Enterprise DLT*

The implementation of permissioned DLT can be achieved using various open-source platforms to support enterprise-grade applications. These applications expect the participants to be identifiable while simultaneously maintaining the privacy and confidentiality of the transactions. They also demand better transaction throughput with considerably lower latency. A permissioned DLT counterbalances these requirements with its key characteristics of variable decentralization, defined roles, privacy, and controlled access. This synergy gives rise to enterprise DLT. The term enterprise DLT is used in industry parlance for an enterprise-grade application deployed on permissioned DLT and is adopted in this paper to associate practitioner terminology with formal literature [65].

At the outset, ethereum was tailored to serve these business needs of the organization [66]. In public DLT, ethereum follows the proof-of-stake consensus mechanism, which requires substantial tokens that can be staked to validate the transactions. Meanwhile, these do not offer a feasible option. proof-of-authority was introduced, where validators are elected, and their public key is stored in the genesis block and is trusted based on off-chain management [67]. This off-chain management affects the privacy of transactions and raises concerns about data visibility. Additionally, ethereum also faces challenges related to inconsistent throughput and latency in adversarial situations [68].

Considering the concerns of Identity Management and the lack of flexibility and privacy, the open-source enterprise DLT platform, hyperledger fabric, was developed by the Linux Foundation [69]. The data in these DLTs is stored in the organization's preferred database management system, and every transaction activity is logged onto the ledger of the DLT, making it immutable and transparent at the same time. These ledgers are append-only, and every record on these ledgers is cryptographically secured, making them immutable [70]. DLT has transformed the traditional ledgers that were used by business merchants and banks for record-keeping of various business activities like financial transactions, inventory, and other business logs into a digitized and decentralized ledger that safeguards data from illegitimate manipulation [8].

### *3.4. Analyzing Enterprise DLT Perspective on Hyperledger fabric*

In this enterprise DLT, the organizations can form a consortium network with their peers and clients. These peers are identified using Public Key Infrastructure issued by the Certificate Authority of each organization. Hyperledger fabric offers the flexibility for organizations to share a Certificate Authority as the only trusted source for issuing identities for the network, or each organization can have its own. These identities also consist of the roles and privileges assigned to each peer in the form of an X.509 Digital Certificate. The identities are then verified at every step with the help of a membership service provider (MSP) [71].

A client application is a user interface that queries the database; these queries are identified as transactions on the network. These transactions can be as simple as a read request to extract a view of

the database, or may include write requests to add, delete, or modify data in the database [72]. To execute the transactions, a software program is required, and in hyperledger fabric, it is referred to as chaincode [73]. Chaincodes are written as a set of functions that allow controlled access to the ledger. These chaincodes are initialized and installed on the channel [74]. A channel can be simply understood as a secure communication between the peers in a network. The transaction performed via the chaincode on the channel remains private to the channel members, ensuring privacy and transparency to the channel members.

These chaincodes can be written in the following languages: Go, Java, and Node.js. These chaincodes ensure that the client is identifiable and that the endorsing peer endorses every transaction proposal submitted in accordance with the defined endorsement policy [75]. The endorsement policy defines the number of peers that can endorse a transaction proposal. These policies can be defined using AND, OR, OutOf, or at the Key-level. For instance, in a supply-chain scenario, the endorsement policy determines the number of organization peers that can create an asset. In figure 5, endorsement should be done by a peer of organization Org1, or peers of organizations Org2 and Org3.

```
Policies:
    Endorsement:
        Type: Signature
        Rule: "OR('Org1MSP.member', AND('Org2MSP.member', 'Org3MSP.member'))"
```

**Figure 5:** Configuration of nested endorsement policy combining AND and OR.

The endorsing peers thoroughly verify the proposal for the identity of the client, the transaction status (new or repetitive) to avoid replay attacks, and that the current state of data in the ledger matches the one presented in the proposal. The proposal is thus signed and returned to the client with verification details and read/write set.

Now, the role of ordering service comes into play. The ordering service receives the proposal from the client, including all verification details, the channel ID, and the permissions granted to create the block of transactions [76]. This service is managed by orderer nodes to achieve consensus using Raft [77]. In DLT, ordering the transactions is crucial as it affects the data commits. In public DLTs, any node can participate in achieving consensus, making it more vulnerable to data faults, which can lead to the forking of the blockchain. Forking cannot be allowed for enterprise-grade applications. On the contrary, hyperledger fabric employs a more sophisticated approach for consensus, that is, the raft consensus algorithm [78].

Raft associated with reliable replicated redundant and fault tolerant properties, is a type of crash-fault tolerance consensus algorithm that assures that consensus will be achieved even if some of its nodes crash. In the Raft-dependent ordering service, the orderer nodes follow an election process to elect the leader that manages the ordering service in the network. Each orderer node initially is identified as a follower and later promotes itself to a candidate based on votes [69]. Each channel conducts its own election process to elect the leader. The orderer nodes of the channel, which are initially in follower mode, will participate in this voting process and request votes from the fellow follower nodes of the channel. The node with the quorum votes is elected as the leader. The leader then accepts the transaction logs assembled in chronological order by channel IDs and adds them to the block. The leader replicates the same block to the followers, which are then delivered to all the peers of the channel. The peers validate the block according to the endorsement policy, and the valid blocks with write permission are appended to the ledger. The block is then committed to the blockchain of every peer on the channel [69].

The activity diagram in figure 6 shows the complete hyperledger fabric transaction flow discussed in this section. The entire process of managing transactions efficiently with decentralization and transparency while maintaining privacy and immutability in hyperledger fabric makes it more appropriate for enterprise-grade applications.

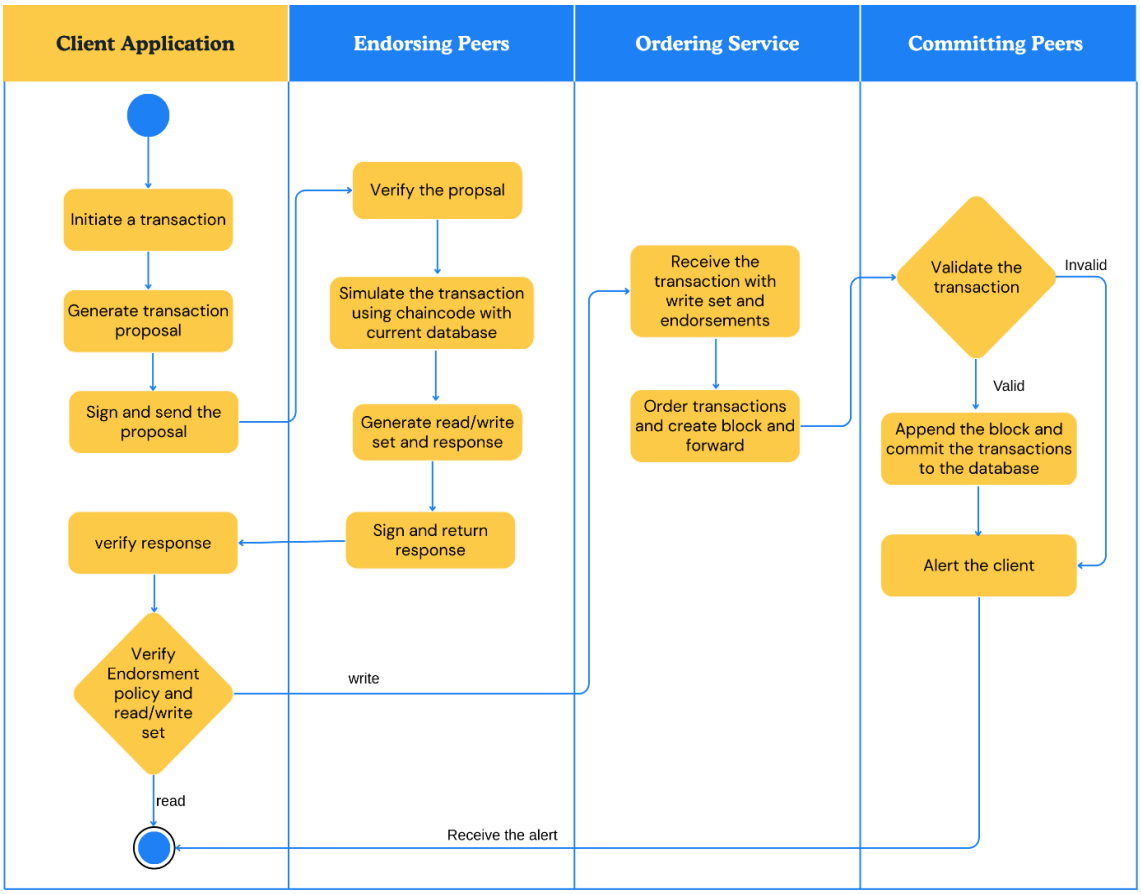


**Figure 6:** Activity diagram for transactions on hyperledger fabric.

### 3.5. *Multidimensional Analysis of Enterprise-Grade Applications*

Table 1 lists the recent research published by various researchers on diverse enterprise applications deployed across multiple well-known DLTs. The table also highlights the limitations of all the proposed models and frameworks. The significant limitations observed in various use cases or application domains are: a) They are implemented on permissionless networks or test networks; b) privacy concerns are partially addressed; c) slowing down decision-making because of too much transparency; d) lack of scalability in experiments and evaluation for a few models; e) all transactions are linkable, intruding on the user's privacy.

**Table 1:** Critical and independent analysis of enterprise-grade application across various use cases (2023-2025).

| Ref | Enterprise-grade application use case | Key Contribution | Limitation |
|---|---|---|---|
| [37] | Supply chain management | A resilient supply chain management with controlled visibility | Implemented on Tendermint, a permissionless blockchain, resulting in excessive transparency to all stakeholders, hindering decision-making and privacy risks, and can be built using Hyperledger Fabric |
| [69] | Unmanned aerial vehicle governance | Offers a solution to monitor unmanned aerial vehicles for violation detection by the regulatory authorities. | Does not support the governance requirement across countries, resulting in interoperability issues with privacy and security concerns. |
| [74] | Generic | A novel model that suggests a hyperledger fabric design based on the user-provided requirement inputs. | The model does not offer support for chaincode and policies. |
| [76] | Healthcare data sharing | A test network on hyperledger fabric to address the fragmentation issue of medical records shared between two medical institutions. | This is a test network with a limited number of workers involved, as it was affecting the latency. The network needs to be tested for scalability in a real-world setting. |

**Table 1:** continue.

| | | | |
|---|---|---|---|
| [79] | Decentralized identity | Fully anonymous decentralized identity supporting threshold traceability with practical blockchain. | The application expects the system to track every financial transaction initiated and maintain complete audit logs for review in case of any fraud. Making these identities traceable results in major privacy issues, which should be addressed to make the system more efficient. |
| [80] | Healthcare information management | With the use of Secure Multiparty Computation (SMPC) and additive homomorphic encryption, the model offers a secure and confidential access to anonymized EHR. | The computations in these encryptions are complex and can be extended further by using fully homomorphic encryption. |
| [81] | Internet of things | A strategy to implement Remote Patient Monitoring using Blockchain with encrypted data storage and exchange. | The strategy focuses on in-depth data storage and exchange by incorporating encryption techniques, albeit at the cost of compromising patient privacy for every data exchange. |
| [82] | Customer relationship management | A framework that offers traceability for client requirements and allows all stakeholders to track all tickets raised. | The framework performance can be optimized for better chaincode execution and stimulate sustainability by supporting integration with existing Enterprise Resource Planning systems. |
| [83] | Business modelling | A decentralized business modelling that focuses on Privacy Information Retrieval during the planning phase, as business modelling requires it for planning profitable strategies. | Computational complexity for cryptographic activities is hindering the performance of this model and can be optimized. Zero-knowledge proof can be implemented. |
| [84] | Smart home communication | A multi-chain smart home application to monitor the environment through sensors. The framework is designed with a private ethereum blockchain at the fog layer and hyperledger fabric at the cloud layer. | The multi-chain framework is not optimized for large-scale networks and sensor data. |
| [85] | Meteorological monitoring system | The framework monitors the weather information received from 4 sensor parameters and is validated, while maintaining the privacy of sensitive validation data. | Infrequent data and few validation parameters are used for evaluation of the model. Cross-chain integration with parallel processing of validation components as the system uses fixed batch size for processing the transactions. |
| [86] | Agricultural system | Designed a framework to protect agricultural biological risk data from manipulation using proxy reencryption technology. The traceability addresses the challenges related to sustainability. | Hardware requirements for the data owner to perform encryption and re-encryption keys will affect the model's performance by increasing response time and CPU utilization. Optimizing these requirements can lead to improved performance. |
| [87, 88] | Education | A distributed system for issuing and verifying academic credentials of students. This is built using Self-Sovereign Identity SSI for identity management and EOSIO blockchain for storage. [95] is another implementation for SSI on ethereum and Hyperledger Besu. | The system should provide support for wallet recovery and be both cost-effective and interoperable. [95] is implemented on ethereum-based chains and presents scalability and off-chain trust, raise privacy concerns. |
| [89] | Web of things | The approach focuses on IoT interoperability by leveraging Web of things. hyperledger fabric is used to create digital twins. | The state of the IoT device is currently not saved on the ledger and is contacting the web of things gateway for this activity. The response time can be improved by storing state on the blockchain. |
| [90] | Renewable energy communities | This experiment focuses on addressing the incorrect data reporting to the communities by deploying chaincodes with well-defined policies on hyperledger fabric. | This experiment is conducted on sample data and should be tested on real-time data to obtain the actual performance evaluation results. |
| [91] | Insurance claim for medical prescription | An AI-assisted blockchain framework that enables prescription generation with the patient as the owner who grants access to various associated entities for smooth insurance claims, utilizing access controls and proxy re-encryption. | The access control mechanism is not clearly defined, though it is implemented. Also, the mitigation strategies for proxy re-encryption are not explicitly mentioned. Additionally, local implementation on Ganache does not address the Gas limit concern in real-time. |

**Table 1:** continue.

| | | | |
|---|---|---|---|
| [92] | Multimedia system | An architecture based on hyperledger fabric with Swarm for storage of multimedia content. The combination enhances the security of content from misuse and other manipulations. | This architecture is not scalable and focuses on the personal multimedia content of an individual. This needs to be tested for large Multimedia content. |
| [93] | Data catalog vocabulary datasets | A blockchain-based model that creates persistent IDs for data catalog vocabulary records to handle the broken link and single point of failure. | Off-chain governance for identity approval. |
| [94] | Land Registration | A model built on Hyperledger Iroha because of the multisignature feature. This enables the registration and transfer of land with the approval of a single or multiple owners. | Not tested for scalability and does not demonstrate implementation of the government policies. |
| [95] | Microbial data sharing | A prototype to share microbial data between different entities with very limited features. It is to be implemented on hyperledger fabric. | It is a prototype that does not utilize the chaincode for efficient access control. |
| [96] | Meta-operating system | A research project that is built on Various platforms AI, IoT, Hyperledger Indy, Federated Learning, and Edge Computing. The project aims to offer secure logging and decentralized trust management. | As this project is a combination of different technologies, decentralization is not enabled at every layer. Also, there will be challenges related to usability and implementation. |
| [97] | Health care system | A chaincode-based access system to maintain the anonymity of the clients during chaincode transactions. | This model claims to use Idemix for anonymization, but uses X.509 credentials, which leads to linkability of every transaction, undermining the goal of the experiment. |

With the comprehensive discussion so far, the RQ 1.1 related to enterprise DLT is strongly answered with reference to various studies conducted in building enterprise-grade applications on various DLTs.

It is noteworthy that many enterprise-grade applications are being deployed on hyperledger fabric; it is evident that these implementations are still in their infancy. The transparent, immutable, and decentralized nature of hyperledger fabric makes it the preferred DLT platform to handle various business workflows of Enterprise DLT. A common concern observed across various proposed solutions is the accessibility, accountability, and auditability of the data involved in the transactions. Hyperledger fabric offers support for this concern with configurable Access Control Lists that define policies for resources. The following subsection discusses the Access Control Mechanism in detail, as it is an integral part of data visibility and addresses RQs 2.1 and 2.2.

### *3.6. Access Control Mechanisms*

Enterprise-grade applications digitize the data under study with a centralized system that monitors all the communication. This digitized data needs to be secured from manipulation, illegitimate access, and a single point of failure. Various technologies are used to address these challenges, but most of them employ a centralized mechanism. DLT provides support for access control, enabling the use of existing policy configurations and defining new policies according to the organization's governance model. Hyperledger fabric has an in-built configuration that deals with access management. As DLT is a peer-to-peer network, it has many features of a network, and an access control list (ACL) [98] is one such feature that comes by default with hyperledger fabric to filter access requests. The organizations that are new to DLT can easily implement their applications on hyperledger fabric with the basic ACL configuration. The focus of this subsection is to carefully understand and present the answers to the RQs identified related to the access control mechanism in sub-subsection 3.6.1. Sub-subsection 3.6.1 provides an extensive understanding of ACL, and sub-subsection 3.6.2 focuses on the other access control models.

### 3.6.1. Access Control List of Hyperledger fabric

Hyperledger fabric is identified as a secure permissioned network due to its certificate authority (CA), MSP, and ACL [99]. To understand this, each component should be analyzed. The CA assigns a unique identity in the form of X.509 digital certificate to every single member. This certificate defines them as admin, peer, orderer, or client of an organization. Figure 7 is a sample of a digital certificate that shows the name denoted as C, OU denotes organizational unit, which defines the role the members play in the organization, and O identifies the organization. This certificate is issued by the issuer CA. The certificates are stored in the MSP directory structure of each participating organization [98].

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 15827340 (0xf1834c)
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = ca.org1.example.com
        Validity:
            Not Before: Oct 24 10:00:00 2023 GMT
            Not After : Oct 23 10:00:00 2024 GMT
        Subject: C = Admin@org1.example.com, OU = admin, O = org1.example.com
```

**Figure 7:** X.509 digital certificate for hyperledger fabric administrator.

There are other fields in the certificate that give details about the keys, issue date, expiry date, and other optional fields, which will be discussed in the following sections. This certificate will be verified by the MSP whenever a client initiates a transaction using a chaincode using the certificate stored in the directory, and the MSP also verifies that the config.yaml file has the NodeOU enabled to read the OU value from the certificate for all types of members. After verification, the certificate will be validated against the policies defined in the ACL [98].

ACLs are the core component of hyperledger fabric's architecture, providing security to the network artifacts defined in the configuration file configtx.yaml, with different sections contributing to policy-making [98]. ACLs facilitate the management of network resources. In hyperledger fabric, resources are either the chaincode operations or events triggered in the network. To manage these resources, policies need to be defined. Policies permit read, write, or administer access. ACLs bind these policies to resources, providing controlled access in the network. These policies are categorized into two types: 1) Signature, 2) ImplicitMeta [98].

The Signature policies are used to identify and validate the users who are allowed to perform specific actions, such as signing the transactions. Figure 8 shows that the Signature policy is defined for Readers, Writers, and Administrators with the rule specified using AND, OR, and NOutOf operators. The rules allow Org1 admin, peer, client, or admin to sign read transactions. Similarly, write permissions are granted to only the admin and the client, whereas administration can be done only by the admin of the organization. Signature policies are configured at the organization level [98].

```
Policies:
    Readers:
        Type: Signature
        Rule: "OR('Org1.admin', 'Org1.peer', 'Org1.client')"
    Writers:
        Type: Signature
        Rule: "OR('Org1.admin', 'Org1.client')"
    Admins:
        Type: Signature
        Rule: "OR('Org1.admin')"
```

**Figure 8:** Org1 access control policies.

ImplicitMeta policies are defined at the channel or application level and depend on the aggregated outcome of the Signature policy of all organizations in the network. If the Signature policies grant access for any transaction, then ImplicitMeta policies will be validated. As this works on the aggregation of

the previous policies, the operators used here are ANY, ALL, or MAJORITY. Policies in figure 9 define that if any reader from any organization in the network have signed it, then permits reading [98].

```
Policies:
    Readers:
        Type: ImplicitMeta
        Rule: "ANY Readers"
    Writers:
        Type: ImplicitMeta
        Rule: "ANY Writers"
    Admins:
        Type: ImplicitMeta
        Rule: "MAJORITY Admins"
```

**Figure 9:** Application access control policies.

Likewise, if any writer signs it, the transaction will be granted. The majority means that if the majority of the admins have signed it, then only it will be accepted; otherwise, the transaction will be rejected. This is a default policy that can be modified according to the organization's requirements. The next step is to bind these policies to resources and create the ACL. ACL binding syntax is presented in figure 10.

```
Application:
  ACLs:
    <binding>: <policy>
```

**Figure 10:** Access control list syntax.

The left-hand side of the colon defines the policies, and the right-hand side of the colon defines the path to the identity that can perform it. Example: peer/propose defines the policy that determines who can submit the proposal to the peer, and /Channel/Application/Writers checks whether the identity of the user who submits the proposal has writer permissions or not, as shown in figure 11.

The entire ACL process is straightforward and easy to implement; however, it does not satisfy all the requirements of enterprise-grade applications. The reasons could be, firstly, the organizational units are limited to admin, peer, client, and orderer. This does not provide the flexibility of assigning different roles according to the requirements of enterprise-grade applications. Secondly, the network-level operations are coarse-grained and pre-defined, which does not allow for defining new ones. Lastly, the ACLs are not dynamic; at their core, they do not allow for defining fine-grained rules of enterprise-grade applications to access specific records, or restrict access if explicit criteria are not fulfilled according to the business logic.

These challenges of ACLs can be addressed through the implementation of access control models, as defined in the next subsection. These models utilize the optional field in the digital certificate and enable a fine-grained access control mechanism [98].

```
ACLs:
  _lifecycle/CommitChaincodeDefinition: /Channel/Application/Writers
  lscc/ChaincodeInstall: /Channel/Application/Admins
  peer/Propose: /Channel/Application/Writers
  peer/ChaincodeToChaincode: /Channel/Application/Writers
  peer/GetChainInfo: /Channel/Application/Readers
  peer/GetBlockByNumber: /Channel/Application/Readers
  peer/GetTransactionByID: /Channel/Application/Readers
  peer/GetBlockByHash: /Channel/Application/Readers
  peer/GetTxEvents: /Channel/Application/Readers
  event/Block: /Channel/Application/Readers
  event/FilteredBlock: /Channel/Application/Readers
  peer/Deliver: /Channel/Application/Readers
  peer/DeliverFiltered: /Channel/Application/Readers
```

**Figure 11:** Access control list configuration.

### *3.6.2. Access Control Models*

Enterprise-grade applications are not always straightforward in terms of their workflow, roles, and operations. It requires a more granular approach to process the transaction request from any end-user, as it involves checking the role, privileges, access levels, and other eligibility criteria. The conventional ACL in hyperledger fabric is restricted to roles with limited network operations. Considering these confinements of conventional ACLs, access control models are introduced in DLT to enhance data security and privacy. These models are adopted from computer networks after identifying their strengths to offer flexibility and build a secure network environment. Each model offers a fine-grained level of security, which is versatile and efficient in handling various transaction requests. These models are categorized as: 1) Role-based access control (RBAC), 2) Attribute-based access control (ABAC), 3) Discretionary access control (DAC), and 4) Mandatory access control (MAC) [24]. The following sections highlight the research on these models for various DLTs and analyze them.

#### *3.6.2.1. Role-Based Access Control*

BRAC empowers the organization to define the policies based on the role and responsibilities assigned to the member, rather than directly to the member [100]. Algorithm 1 presents a simple process of access validation in RBAC. The roles associated with users are retrieved to check for the permissions in the policies, and based on the permissions, access is granted or denied to perform an action on resources. The policies and roles can be defined in functions of smart contracts or chaincodes. These functions can also validate the transaction requests. The organization can utilize predefined roles in the case of hyperledger fabric implementation and define only the necessary policies. The policies defined by organizations are not constant throughout the lifetime of the enterprise. Policies continue to evolve in response to changes in technology, workflows, and the users involved. The enterprise applications should be reviewed on a regular basis, and policies should be renewed [30].

**ALGORITHM 1:** Role-based access control.

```
1: RBAC_Check(User U, Resource res, Action a)
2:     Retrieve roles R assigned to User U
3:     for each role i in R
4:         Retrieve permission P for i
5:         if permission P allows action a on resource res then
6:             return access Granted
7:         end if
8:     end for
9:     return access Denied
```

Salve *et al.* [101] proposed L2DART, an implementation of a role-based trust management system on ethereum to regulate smart contract execution access. This model utilizes Python for off-chain computation, as it consumes a good amount of gas as a transaction fee to verify the role in its predecessor model. On the other hand, Sivakumar *et al.* [102] proposed role-based event driven hybrid framework that allows defining policies and roles for academic publications. This framework was tested for 10,000 publications, which limits access based on the responsibility assigned to each role. Cryptographic computations and storage of documents were done off-chain to optimize transaction costs.

A framework with a hybrid access control policy, where all four types of access control models were combined for financial institutions, was proposed by Daah *et al.* [103]. This framework was deployed on the ethereum Ganache blockchain. The policy decision point evaluates the transaction request received and enforces the policies based on role, attribute, discretionary permissions, and mandatory controls. The deployment in a personal blockchain, such as Ganache, is different from the actual ethereum blockchain in a real-world financial setup. This model will incur a large transaction fee and needs to be optimized.

In hyperledger fabric, the organizational unit field in the digital certificates identifies the role of a member, which is restricted. Zaidi *et al.* [104] presented a flexible model where roles and policies can be flexibly defined in the chaincode. It also attempts to address the issue of when a user is associated

with more than one role. In such cases, the chaincode function validates the request by taking the union of the permissions for the roles assigned to the user and grants access. This model performs fairly well with a limited number of users; however, it has not been tested for scalability or in real-world situations, such as concurrent user requests. Additionally, the model does not explicitly check for the accuracy and consistency of the rules defined. Sutradhar *et al.* [105], proposed an identity and access management system that is designed by integrating OAuth 2.0 to handle authentication and authorization. Using a third-party application to balance the load on the Fabric and improve the performance is good, but at the same time, there is always a risk with third-party applications being compromised or incompatible. Hyperledger fabric's modular architecture can handle multiple tasks efficiently. A similar approach was presented by Ouaddah *et al.* [106]. The role-based access model can be strengthened by using more granular policies and roles, as hyperledger fabric is capable of handling the identities.

LedgerView, was designed to manage views generated by specific queries on the data. In this system, Ruan *et al.* [107] used hyperledger fabric to present a controlled ledger view, where access to these views is granted based on the roles defined. For sensitive information, encryption-based access permissions are integrated with RBAC to ensure privacy and confidentiality. This model can be further enhanced by avoiding off-chain encryption computation, making it more secure and auditable.

Makhdoom *et al.* [108] proposed a secure, privacy-compliant distributed framework deployed on oorda permissioned DLT, which uses semi-homomorphic encryption to secure personal identification information. The reason for deploying this on Corda is to guarantee confidential confirmation between nodes sharing the same medium. The user uses semi-homomorphic encryption to secure the required information and grants access to specific roles. This model is designed to handle data from IoT devices for the specific scenario. The data is stored on the cloud, and access is granted using the RBAC model, which may not scale well for a large enterprise-grade application, as consensus is notary-based and may incur infrastructure costs. Also, corda is not a traditional blockchain and lacks transparency and immutability. This DLT is suitable for financial applications and use cases where privacy is the major requirement.

#### *3.6.2.2. Attribute-Based Access Control*

ABAC is the most widely used access control model because of its fine-grained approach, which does not restrict the policy only to roles but also to other possible attributes. Algorithm 2 presents the comprehensive steps involved in ABAC, where a combination of attributes is evaluated to grant access. For example, in an enterprise-grade application for an organization, there can be a role manager with multiple instances. Each manager is supposed to have different access depending on their department. For such a scenario, ABAC allows linking these additional attributes to each role, differentiating their access. These attributes can be defined in the digital certificate or can be defined in the smart contract or chaincode [109].

**ALGORITHM 2:** Attribute-based access control.

```
1: ABAC_Check(User U, Resource res, Action a, Env e)
2:      Retrieve attributes Attr_U  of User U
3:      Retrieve attributes Attr_res  of Resource res
4:      Retrieve attributes Attr_e  of Env e
5:      Evaluate policy on (Attr_U, Attr_res, Attr_e, a)
6:       if policy satisfies then
7:              return access Granted
8:      else
9:              return access Denied
10:     end if
```

AVChain is one of the simplest implementations of ABAC on hyperledger fabric proposed by Singh *et al.* [109]. The framework is used for incident reporting in case of any vehicle crash. As the logs maintained can be tampered with and deleted, they should be accessible only to authorized users. DLT provides better support regarding immutability, privacy, and controlled access. The data storage is done on IPFS as the logs can be of large size and will not be suitable for saving on-chain. Access to these

logs is secured using ABAC policies defined on the chaincode. These access policies can be strengthened by using attribute-based encryption. Peepliwal *et al.* [110], proposed a prototype model to be deployed on hyperledger fabric to handle the data received from wearable IoT devices during the clinical trials. The data is encrypted, and hash values are stored on the block through IPFS. These are validated against the policies and trust levels defined before granting access. The policies are defined for the attributes of sending and receiving nodes to ensure complete trust in the network. This prototype is yet to be implemented.

Sha *et al.* [65] presented ConsortiumSec, a framework designed for consortium blockchain, where ABAC is implemented to enforce access control policies at the consortium level in the network. This model has yet to be fully implemented and tested for various performance parameters. Sarfaraz *et al.* [111] proposed accessChain as another ABAC prototype that was not specifically designed for any blockchain, but proposes to use the global ledger to store transaction logs and validate policies.

Dalabanjan *et al.* [112] proposed a system that provides security against a single point of failure issue with the implementation of ABAC for OpenStack cloud resources with the help of smart contracts. The system is deployed on ethereum and proof of stake as the consensus mechanism for efficient performance. This model was tested for scalability and showed good results. Roy and Ghosh [113] proposed a blockchain-based secure access control that implements ABAC with policies defined for device-to-device and user-to-device to control access to information, as the devices can share the data for further processing and evaluating the performance of IoT devices.

Blockchain-based proxy re-encryption access control is a framework proposed by Wang *et al.* [86] for handling test results of agricultural products, specifically information related to biological risk factors. Proxy re-encryption is a cryptographic scheme that allows a proxy to re-encrypt the sender's encrypted message using the re-encryption key derived from the sender's private key and the receiver's public key. The center safeguards the test results from unauthorized access using ABAC. These reports are encrypted with the center's public key, and the hash value is stored on-chain. Each access request is validated against the policies using attributes of the requester, product, environment, and operations. Upon successful validation, the center will re-encrypt with the requester's public key and make the key and the ciphertext available on the blockchain, offering confidentiality and concurrency. This framework can be enhanced by granting the data owner proxy-encryption rights while safeguarding the requester's attributes to avoid the risk of the proxy being compromised, thereby preserving ownership and ultimately satisfying the data visibility concerns.

Wu *et al.* [114] proposed an ABAC scheme to address the data visibility concerns. The scheme tries to protect the attributes and policies from getting compromised by encrypting them. The attributes of the users are encrypted and stored on the certificate by the CA. This encryption is done using the joint public key of the associated nodes elected by the organization. This encryption hides the attributes and, in turn, hides the entities accessing the data. Meanwhile, the policies are also encrypted and stored on the blockchain smart contract. Any access request calculates the difference between the encrypted policy and the ciphertext of attributes in the certificate. This difference will be used then to grant or revoke access. The encryption and decryption will increase the computational complexity and may create additional overhead. Furthermore, a zero-knowledge proof is also required to be added before committing it to the ledger. This model should be optimized with a more efficient encryption scheme.

Madkaikar *et al.* [115] in their study, focused on the policy modifications that happen regularly in enterprise-grade applications. Whenever a policy is added to the list, the list grows large and takes time for processing. A queuing method was suggested in this paper with the ABAC model that accepts the new policies by holding them in the auxiliary list until the current processing of the access requests queue. The new policies in the auxiliary list are updated in the access policies, and in the meantime, the request queue will be on vacation. Applying the queuing approach is a novel idea for handling access requests and can be deployed on hyperledger fabric, allowing for performance analysis in enterprise-grade applications.

#### *3.6.2.3. Discretionary Access Control*

Under rare circumstances, the enterprise-grade applications are expected to handle access requests manually. In the sense that the administrator grants access to certain modules of the application to a completely random user based on his/her own discretion. DAC was initially introduced in DLT but could not be sustained because it nullified the main feature of DLT, that is, decentralization. DAC completely works on user discretion [25]. These users are the data owners and can grant read, write, and execute access to any other user. This kind of access control is rarely used these days, as data is often available online and poses a security risk. It is suitable for small businesses, and only trusted members are involved. Algorithm 3 illustrates the process by which ACLs defined by owners are evaluated to grant access to resources.

**ALGORITHM 3:** Discretionary access control.

```
1: DAC_Check(User U, Resource res, Action a)
2:     Retrieve ACL of resource res
3:     if ACL contains a policy with user U with permission to perform action a then
4:         return access Granted
5:     else
6:         return access Denied
7:     end if
```

#### *3.6.2.4. Mandatory Access Control*

This model is not suitable for DLT because of its centralized approach. The access rights in this model are provided based on levels of hierarchy within an organization. The higher the level, the higher the access. Algorithm 4 shows a simplified process of validating access using MAC model. This kind of model was introduced to manage access in the military and government, where the rank of an individual decides the level of access granted [25]. This model offers confidentiality in a centralized manner, which can lead to a single point of failure and other major access attacks.

**ALGORITHM 4:** Mandatory access control.

```
1: MAC_Check(User U, Resource res, Action a)
2:     Retrieve security level L_U of User U
3:     Retrieve security level L_res of Resource res
4:     if L_U dominates L_res according to policy then
5:         if action a is allowed by the policy then
6:             return access Granted
7:         else
8:             return access Denied
9:         end if
10:    else
11:        return access Denied
12:    end if
```

### *3.6.3. Comparative Analysis of Access Control Implementation*

Data visibility is critical for enterprise-grade applications, as it is about reading, writing, and executing operations on data. These operations are enforced as policies in the models described in the previous sections. Table 2 analyzes the access control model to understand the impact of the implementation proposed by the researchers. For scalability and concurrent access, the rubric is as follows: a) low represents restricting to predefined artifacts of the configuration; b) medium represents small-scale evaluation of the network; c) High represents large-scale evaluation of the network.

**Table 2:** Implementation analysis of access control models.

| Ref | Platform | Model | Auditable | Scalability | Policy Modification | Concurrent Access | Off-chain Computation | User Anonymization |
|---|---|---|---|---|---|---|---|---|
| **[65]** | Hyperledger fabric | ABAC | √ | Low | x | Low | √Partial | x |
| **[86]** | Hyperledger fabric | ABAC | √ | Medium | x | Medium | x | x |
| **[101]** | Ethereum | RBAC | √ | Medium | x | Low | √ | x |
| **[102]** | Ethereum | RBAC | √ | Medium | x | Medium | √ | x |
| **[103]** | Ethereum | RBAC, ABAC, DAC, MAC | √ | Low | √ | Low | x | x |
| **[104]** | Hyperledger fabric | RBAC | √ | Low | √ | Medium | x | x |
| **[105]** | Hyperledger fabric | RBAC | √ | Medium | x | Medium | √ | x |
| **[107]** | Hyperledger fabric | RBAC | √ | Low | √ | Medium | √ | x |
| **[108]** | Corda | RBAC | √ | Medium | √ | Medium | x | √Partial |
| **[109]** | Hyperledger fabric | ABAC | √ | Medium | x | Low | x | x |
| ***[110]** | Hyperledger fabric | ABAC | √ | Yet to be implemented. | | | | |
| **[111]** | Hyperledger fabric/ Ethereum | ABAC | √ | Medium | x | Medium | x | x |
| **[112]** | Ethereum | ABAC | √ | High | x | High | x | x |
| **[113]** | Hyperledger fabric | ABAC | √ | Medium | x | Medium | x | x |
| **[114]** | Hyperledger fabric | ABAC | √ | Medium | x | Medium | x | √Partial |
| **[115]** | Platform-independent | ABAC | √ | Medium | √ | Medium | x | x |
| **[116]** | Hyperledger fabric | VC & DID | √ | Medium | x | Medium | √ | x |
| ***[117]** | Hyperledger Aries | ABAC | Under research | | | | | |
| **[118]** | Hyperledger fabric | ABAC | √ | High | x | Medium | x | x |

*[110] and [117] present a prototype and a conceptual model, respectively, and hence lack evidence for analysis

In DLT, the data is decentralized, disseminated, and transparent to all the users involved in a network, which strongly highlights the concern related to data visibility. Data visibility deals with comprehensive access to data, which includes reading, appending, updating, and deleting. These operations should be monitored in detail in data visibility to ensure accountability and auditability. To achieve this comprehensive access, the access control mechanism plays a vital role [24, 26, 50, 119-122]. The complete discussion in this subsection responds to RQs 2.1 and 2.2 through complete analysis and interpretations of studies conducted and published thus far. This subsection presents strong empirical evidence of how different models and encryption schemes lay a strong foundation for data visibility. The next crucial identity that needs privacy is the user, as presented in table 2. The concern related to user identity is that every transaction is linkable, as the credentials are transparent to and traceable by all the network members. The solution for this is anonymization, which is RQ 3.1 of this study, followed by RQ3.2 to analyze its implementation on hyperledger fabric. The following subsection 3.7 discusses anonymity, which is the second key parameter of data visibility and response to RQs 3.1 and 3.2.

### 3.7. *Anonymity*

In access control mechanisms, the primary focus was on the data, the access rights defined, and how well they are monitored. Very few research publications have focused on the privacy of users who own or request access to data. It is evident from the studies that user identity protection was given the last priority, and researchers are now focusing on this aspect. The identity of the user is equally significant to the data for enterprise-grade applications and for efficient data visibility.

In DLT, every transaction is recorded in the ledgers and distributed to achieve transparency and traceability. This is possible with the use of cryptographic identification for the user, also referred to as pseudonymity [123]. The use of pseudonyms like cryptographic ID in ethereum or X.509 certificates in hyperledger fabric for the real-world entities always poses a threat to the identity of the user, as the identities available in the records can be easily tracked for the kind of transactions a user performs on the DLT, and can be traced back based on the pattern [124]. These identities should be guarded for complete privacy preservation of the user and the data.

Anonymity plays a crucial role in ensuring a privacy-preserving mechanism in DLT. It refers to completely guarding or anonymizing the user's personal details and attributes in such a way that a user can perform transactions without revealing any linkability. Enabling anonymity not only helps hide user details for executing transactions but also provides assistance for secure data sharing. Data Sharing is required for many instances, such as Electronic Health records for research in medicine, or status tracking in supply chain management [125]. This information should be shared with complete confidentiality by hiding the metadata. Metadata here refers to the identity details.

DLT promotes a trust-based environment by providing transparency and traceability through the forfeiture of the privacy of the user [126]. Enterprise-grade applications cannot solely rely on decentralization and accountability; they must also provide strong security for the privacy of all actors involved. Subsection 3.6 presented various mechanisms to control access; likewise, this subsection will present the different tools and techniques that can be utilized in the DLT to make it a privacy-preserving technology.

Zero-knowledge proof (ZKP) [127] is a cryptographic method that achieves anonymity and privacy. ZKP is used to validate the data and user identity without revealing the data and identification details. In ZKP, the two main actors are the prover, who proves the validity of data and identity, and the verifier, who should be convinced [128]. This interaction does not reveal any information even to the prover, which makes ZKP the most suitable technique for a privacy-preserving mechanism on DLT. ZKP is classified as an interactive and non-interactive ZKP [31, 32] as shown in figure 12.

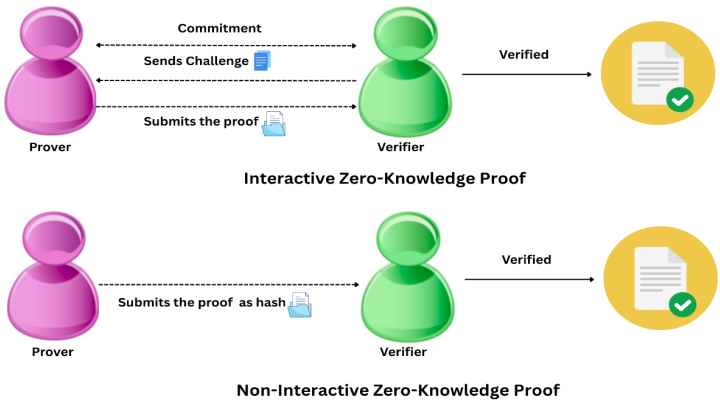


**Figure 12:** Graphical representation of zero-knowledge proof.

An interactive ZKP establishes a communication line between the prover and verifier, comprising three phases. The first phase expects the prover to generate a proof and forward it to the verifier. The second phase is the challenge phase, where the verifier presents random challenges for the prover, and in the last phase, based on the responses, acceptance or rejection occurs. These interactions are prone to replay attacks, where an attacker uses one of the valid proofs to interact with the smart Contract and gain access [31].

To mitigate these attacks, a non-interactive ZKP was introduced, which involves only a single communication. In a non-interactive ZKP, the prover generates a proof and shares it as a cryptographic hash with the verifier, which can be checked later. This ensures a single secure message is shared to avoid multiple interactions and replay attacks. The non-interactive ZKP is more suitable for DLT, as it helps to avoid additional transaction costs and time. Oude Roelink *et al.* [129] presented a systematic review of non-interactive zero-knowledge proof (NIZKP) protocols, specifically zero-knowledge succinct non-interactive argument of knowledge (Zk-SNARK), zero-knowledge scalable transparent argument of knowledge (Zk-STARK), and bulletproof. Table 3 below highlights and compares the features of anonymity and privacy-preserving protocols used in DLT. Anonymity can be achieved in DLT when the protocol adopted is scalable with a small-sized proof that takes an optimal amount of time for verification. These protocols are also expected to be secure against attacks. For enterprise-grade applications, these features are essential to safeguard the security and privacy of the users, nodes, and data.

**Table 3:** Comparing anonymity and privacy-preserving protocols.

| Feature | IZK | NIZK | Zk-SNARK | Zk-STARK | Idemix |
|---|---|---|---|---|---|
| **Communication** | √ | x | x | x | √ |
| **Trusted Setup** | x | Partial | √ | x | x |
| **Transparency** | √ | Partial | x | √ | √ |
| **Post-Quantum capabilities** | x | x | x | √ | x |
| **Proof Size** | Large | Medium | Very Small | Large | Small |
| **Verification time** | Slow | Fast | Fast | Fast | Fast |
| **Scalability** | x | Partial | Moderate | High | High |
| **Blockchain Application** | x | Bulletproofs, Monero | Ethereum- Zcash | StarkNet | Hyperledger fabric |
| **Tools** | Proof Assistance | Dalek | ZoKrates, Circom | Cairo | Idemix |

√ denotes supported and x- denotes not supported. Post-Quantum variant of these protocols is under-researched.

Ben-Sasson *et al.* [130] proposed Zk-SNARK as an optimized solution to implement non-interactive ZKP. It generates shorter proof that takes less time for verification, which makes Zk-SNARK suitable for DLT. Zk-SNARK requires a trusted setup in the initial stage, where a secret reference string, prover, and verifier keys are generated. These keys are later used for generating and verifying the proofs. Elliptic-curve cryptography and pairing-based checks are utilized to generate the smaller keys and shorter proofs, thereby enabling efficient performance.

Though Zk-SNARK uses a smaller proof, it is risky with regard to the initial trusted setup. The reference string used to generate the key pairs should be securely discarded. To overcome this risk, Ben-Sasson *et al.* [131] introduced Zk-STARK, which does not require any trusted setup and is entirely random. This randomness makes Zk-STARK transparent and scalable, resulting in faster verification and improved scalability and performance. On the contrary, Camenisch *et al.* [132] proposed Idemix anonymous credentials, which provide both anonymity and unlinkability simultaneously, require no trusted setup and support selective disclosure. Table 4 presents a comparison of anonymity-related studies on DLT using ZKP.

Web 3.0 centers around decentralization and transparency, making it an archetype of DLT. These characteristics of Web 3.0 allow users to create multiple accounts without authentication on the DLT. Wang *et al.* [133] proposed a zero-knowledge Blockchain-based decentralized Identity system to address this issue by linking souls to humans. The system uses a Zk-SNARK program off-chain to prevent the creation of fake or additional accounts by using the valid secret credential and its public hash. The trusted setup and the one-to-one mapping of Blockchain Identity with credentials via linkable ring signature result in linkability and privacy issues. Zhao *et al.* [134] proposed a ring signature scheme. A ring signature is a digital signature that uses all the public keys, used for signing on behalf of the group without revealing the actual public key associated with the private key. For certification, a key image is generated using the ring and the private key on the account address. The smart contract later verifies the image with the ring and the address by traversing its storage for duplication and certifies it. This

ring signature check guarantees that only one account can be signed by a single user. This entire system was deployed on the ethereum test network and will need to address the challenges of high gas cost, latency, and scalability. This system also involves off-chain computation, which increases the processing time. A better choice of DLT can be made to overcome these performance issues.

Keršič *et al.* [135] present the zero-knowledge machine learning (ZKML) framework to ensure data privacy using Zk-STARK. The verification is done on-chain with a Cairo smart contract on the Starknet network for proof generation, and on the ethereum mainnet, proofs are verified using Zk-STARK. This model needs to be reviewed and improved to provision machine learning models, as they require heavy computational graphics processing unit support. Heo *et al.* [136] addressed the privacy issue at the foundation of blockchain, which focuses on the storage of the entire ledger on full nodes. Non-interactive practical proof-of-storage is designed to verify whether full nodes are storing the complete correct ledger. Zk-STARK enables any node to verify this storage on the network, making it decentralized and resistant to sybil attacks. J *et al.* [137] proposed a secure endorsement mechanism on hyperledger fabric, with a major weakness in the trust assumption for the client and the policy creator, along with linkable threshold ring signatures.

**Table 4:** Comparing ZKP approach and anonymity mechanism on DLT.

| Ref | Platform | Approach | Anonymity Mechanism | Key Limitation |
|---|---|---|---|---|
| **[97]** | Hyperledger fabric | Chaincode-based access control | Claimed to implement Idemix | No clear proof of implementation of Idemix for anonymity and unlinkability. |
| **[128]** | Ethereum | Address abstraction scheme for mapping web2 identities with web3 | Zk-SNARK with ZoKrates to offer unlikability | Credential revocation is not supported. Certificates are bound to a trusted anchor, making the model unreliable. |
| **[130]** | Custom Virtual Machine | Non-Interactive ZKP | Shorter proof for faster verification with trusted setup | Trusted setup required for generation of key pair is a major limitation of this model as it can be compromised. |
| **[131]** | General Purpose | Non-Interactive ZKP and Interactive ZKP transparent approach | Randomness with no trusted setup | Larger proof size and relies on randomness for non-interactivity. |
| **[132]** | General Purpose | Non-Interactive ZKP | Idemix Anonymous Credentials | Anonymity depends on the support provided by the implemented network model. |
| **[133]** | Ethereum with Web 3.0 | Zero-Knowledge Blockchain-based decentralized Identity | Zk-SNARK | Mandatory trusted setup with a linear increase in cost with ring size. |
| **[134]** | Generic DLT | Logarithmic-size revocable ring signatures | Ring signature with linkability | Lack of support for enterprise-grade applications as on-chain revocation checks increase latency. |
| **[135]** | Ethereum | Zero-Knowledge Machine Learning combining Halo and Orion ZKP frameworks | Computational privacy using Zk-STARK transparency and Zk-SNARK trustless setup | Limited performance analysis with results restricted to public DLT. Anonymization is restricted to data and not the user, making the model linkable. |
| **[136]** | Generic DLT | Non-interactive Practical Proof-of-Storage | Zk-STARK for public storage verifiability | User and transaction anonymization is not considered compromising the security and privacy of the user. |
| **[137]** | Hyperledger fabric | Linkable threshold ring signature | Anonymous endorsement with Zk-SNARK, RSA accumulator for batch verification and Commit-and-Prove zk-SNARK | Not tested for user and transaction support. MSP leakage is partially addressed, leading to linkability. |
| [138] | Data Network (no DLT) | Encryption and Re-encryption without ZKP | Not Implemented | Analyzed Access Control Mechanisms |
| **[139]** | Cloud (no DLT) | Lightweight Authentication | Rotating Confidential Privacy | Limited Anonymization |
| **[140]** | Cloud / IoT (no DLT) | Multifactor Authentication with lightweight Cryptography | No Anonymization | No proper Anonymization of user, peer, or transactions. |

**Table 4:** continue.

| | | | | |
|---|---|---|---|---|
| **[141]** | WSN/ IoT (no DLT) | Multifactor Authentication with forward secrecy | Session key agreement with forward secrecy | No proper implementation of Anonymity and ZKP |
| **[142]** | Cloud (no DLT) | Improved Authentication for remote data access | Improved challenge and response authentication | No proper implementation of Anonymity and ZKP |
| **[143]** | General Purpose | ZKP for set membership | Succinct ZKP | A theoretical approach and lacks implementation. |

Other studies proposed a mixed approach, as Nour *et al.* in [138] identified, categorized, and investigated different access control mechanisms that can be deployed in a data network to validate the access control policies for authorized data access. Chaudhry *et al.* [139] proposed an authentication scheme for an IoT environment that can withstand security attacks with better performance. Atiewi *et al.* [140] proposed a method that separates sensitive and non-sensitive data, which is stored in private and public clouds, respectively. To ensure authorized access, Wang *et al.* [141] used advanced encryption standard in the private cloud and three-level multifactor authentication in the public cloud. Ghaffar *et al.* [142] proposed an improved authentication protocol that withstands different security attacks. Benarroch *et al.* [143] proposed CP-SNARK using a rust library for anonymous credentials.

Based on the discussion so far, anonymity is not a built-in feature of permissioned DLT, especially hyperledger fabric, and requires integration using protocols and tools compatible with permissioned DLT. Idemix is well-suited to the hyperledger fabric architecture and does not officially support any other DLT [97].

The study thus far has answered the RQ 3.1 and RQ 3.2 with a detailed explanation of anonymity, along with its significance, and various cryptographic approaches that lay the strong foundation for anonymity and linkability in DLTs like ethereum and hyperledger fabric.

## 4. Discussion

Data is always a primary focal point for any application in the continuously evolving technological realm, where it is available at the fingertips anytime, anywhere. Shielding this data is an incessant activity that should be sophisticated and optimized spontaneously or consciously. These data protection measures can be summarized in a single term, the data visibility. Data visibility signifies the ability of an organization or group of organizations to govern, access, and understand data to process in real-time or quasi-real-time. It enables the organization to make informed decisions, optimizing performance, and ensuring compliance. These can be managed with an efficient enterprise-grade application that monitors the stakeholders, analyzes activities, and mitigates risks. Various tools bundled with DLT offer tremendous advantages for Enterprise DLT.

From a research perspective, the study reveals that enterprise-grade applications can be built on hyperledger fabric owing to its exclusive features of decentralization, transparency, security, privacy, and pluggable consensus mechanism. These applications will involve rigorous transaction activities that require the system to perform all actions in an optimal timeframe for improved results and end-user satisfaction. ethereum is not ideal for implementation due to the high gas cost associated with every transaction; however, Layer-2 solutions such as Optimistic Rollups, zkEVM with Quorum, and Hyperledger Besu [101] mitigate these gas limit constraints. In addition, with every cryptographic activity, the computational overhead will proportionally increase the gas cost [83]; to address this, off-chain computations are suggested, which create additional hardware overhead for the user. Furthermore, it is evident that access control mechanisms can only be implemented using smart contracts. The smart contracts in ethereum have certain limitations in performing these activities, and to address this, many researchers have opted for off-chain computation [27, 28, 43, 144]. Also, the validation of access policies in ethereum was distributed, which directly impacts data visibility. Although the support for data visibility is implemented and evaluated to a great extent, it does not guarantee scalability and efficient performance [129].

Conversely, the implementation on hyperledger fabric was scalable and efficient, particularly in terms of deploying the access control models and managing the data visibility throughout the network. Hyperledger fabric has conventional access control support that can be utilized for small organizations. For a large enterprise, access control models can be implemented through chaincode. The implementation of access control models was extensive and has outperformed ethereum with regard to throughput and latency. This presents a strong validation that data visibility in enterprise-grade applications can be efficiently controlled if deployed on hyperledger fabric. Alongside data access control, the anonymity of the members involved in the transaction is also vital [80, 145]. Various studies have been conducted and evaluated primarily on ethereum [140]. The studies included diverse zero-knowledge proof protocols that are essential for privacy preservation in the network. Zk-SNARK and linkable ring signatures have been presented in various models, but they often lack scalability or require off-chain computation for optimized performance. Idemix and Zk-STARK were among the few empirical implementations on hyperledger fabric with considerable scope for improvisation and evaluation. Idemix is restricted to anonymizing only the client, and Zk-STARK requires expertise and knowledge for integration.

Another major limitation observed in most of the studies is a lack of support for scalability. The models were not assessed for concurrent transactions, which are expected in an enterprise-grade application. The ones that are tested are with a limited number of organizations and nodes. Faster Computation, scalability, and concurrent secure transactions need to be analyzed to develop an efficient enterprise-grade application with controlled data visibility.

## 5. Conclusions

This paper presents a systematic literature review that analyzes and evaluates solutions proposed by various researchers to address enterprise-grade application concerns during the period (2023-2025). The paper analyzed 123 publications and identified DLT as the most suitable technology for enterprise-grade applications. Additionally, the term Enterprise DLT is devised in this literature, presenting a comprehensive approach for identifying enterprise-grade applications deployed on permissioned DLT.

The security concerns on Enterprise DLT led to an investigation into data visibility. Data visibility has always been a critical concern in any enterprise-grade application with multiple stakeholders, as it is not restricted to mere viewing of the data, but it involves multiple significant factors such as defining stakeholders, resources, access policies, and other artifacts. These artifacts should be governed by security protocols that ensure data privacy and the privacy of the stakeholders. This streamlined the research focus to two key parameters of access control and anonymity.

On further analysis of these two parameters, the study identified the longitudinal challenges for efficient data visibility control that include:

- The security and privacy protocols required iterative refinement with technological advancements.
- The areas that are significantly under-researched include handling selective disclosure, support for post-quantum capabilities, and computational overhead management.
- With billions of active users, a scalable solution that adheres to all access policies, with anonymization of every user and guaranteeing unlinkability, poses a formidable challenge.
- With various enterprise DLT platforms, the need for interoperability is predominant for a sustainable DLT.

Besides these, the study highlights the immediate concerns that can be addressed as a precursor to longitudinal challenges:

- Enhancing the scalability in the ABAC Mechanism as it offers a more fine-grained approach compared to the other three Access Control Mechanism.
- Dynamic Access policy modifications on Enterprise DLT.
- Reduce the computational overload for anonymization without adopting off-chain computations, as it sometimes shifts load instead of balancing.
- The studies done so far are isolated in nature, in the sense that they have either addressed access control or anonymity but not both.

A balanced approach for efficient data visibility on hyperledger fabric, a permissioned DLT, is desirable for an enterprise-grade application. This approach can be a coalescence of various mechanisms studied so far in this paper. This coalition model should be deployed on hyperledger fabric with an efficient attribute-based control model that ensures privacy, filters, and audits every transaction request to ensure a secure and decentralized environment. In addition to the access control model, a scalable zero-knowledge proof technique is needed that not only performs on-chain verification quickly but also gradually decreases the turnaround time.

**Author contributions: Afeefa Noorain:** Conceptualization, Formal Analysis, Investigation, Methodology, Validation, Visualization, Writing – original draft, Writing – review & editing. **Khaleel Ahmad:** Conceptualization, Methodology, Supervision, Validation, Writing – review & editing. **Laura Emilia Maria Ricci:** Supervision, Validation, Writing – review & editing.

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

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

**Funding:** The authors did not receive support from any organization for the conducting of the study.

## References

[1] D. Jeong and D. K. Baik, "Incremental data integration based on hierarchical metadata registry with data visibility," *Information Sciences*, vol. 162, no. 3–4, pp. 147–181, Jun. 2004, doi: 10.1016/j.ins.2003.09.008.

[2] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, G. Livraga, and P. Samarati, "Enforcing confidentiality and data visibility constraints: an OBDD approach," in *Data and Applications Security and Privacy XXV*, Y. Li, Ed., Lecture Notes in Computer Science, vol. 6818, Berlin, Heidelberg, Germany: Springer, 2011, pp. 44–59, doi: 10.1007/978-3-642-22348-8_6.

[3] N. J. Ogbuke, Y. Y. Yusuf, K. Dharma, and B. A. Mercangoz, "Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society," *Production Planning and Control*, vol. 33, no. 2–3, pp. 123–137, 2022, doi: 10.1080/09537287.2020.1810764.

[4] F. Shabani-Naeeni and R. Ghasemy Yaghin, "Integrating data visibility decision in a multi-objective procurement transport planning under risk: a modified NSGA-II," *Applied Soft Computing*, vol. 107, art. no. 107406, Aug. 2021, doi: 10.1016/j.asoc.2021.107406.

[5] M. Montecchi, K. Plangger, and D. C. West, "Supply chain transparency: a bibliometric review and research agenda," *International Journal of Production and Economics*, vol. 238, art. no. 108152, Aug. 01, 2021, *Elsevier B.V.* doi: 10.1016/j.ijpe.2021.108152.

[6] I. J. Fraser, M. Müller, and J. Schwarzkopf, "Transparency for multi-tier sustainable supply chain management: A case study of a multi-tier transparency approach for SSCM in the automotive industry," *Sustainability (Switzerland)*, vol. 12, no. 5, pp. 1–24, Mar. 2020, doi: 10.3390/su12051814.

[7] J. Gualandris, A. Longoni, D. Luzzini, and M. Pagell, "The association between supply chain structure and transparency: a large-scale empirical study," *Journal of Operations Management*, vol. 67, no. 7, pp. 803–827, Oct. 2021, doi: 10.1002/joom.1150.

[8] D. J. Ghode, R. Jain, G. Soni, S. K. Singh, and V. Yadav, "Architecture to enhance transparency in supply chain management using blockchain technology," in *Procedia Manufacturing*, Elsevier B.V., 2020, pp. 1614–1620. doi: 10.1016/j.promfg.2020.10.225.

[9] I. M. van Schilt, J. H. Kwakkel, J. P. Mense, and A. Verbraeck, "Dimensions of data sparseness and their effect on supply chain visibility," *Computers Industrial Engineering*, vol. 191, p. 110108, May 2024, doi: 10.1016/j.cie.2024.110108.

[10] A. K. Singh, A. Anand, Z. Lv, H. Ko, and A. Mohan, "A Survey on healthcare data: a security perspective," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 2s, art. no. 59, Jun. 01, 2021, doi: 10.1145/3422816.

[11] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing Application*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022, doi: 10.1007/s00521-020-05519-w.

[12] H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," in *Proceedings - 2014 IEEE International Congress on Big Data, BigData Congress 2014*, Anchorage, AK, USA, Sep. 2014, pp. 762–765. doi: 10.1109/BigData.Congress.2014.112.

[13] M. Mwencha, J. E. Rosen, C. Spisak, N. Watson, N. Kisoka, and H. Mberesero, "Upgrading supply chain management systems to improve availability of medicines in Tanzania: evaluation of performance and cost effects," *Global Health: Science and Practice*, vol. 5, no. 3, pp. 399–411, Sep. 2017, doi: 10.9745/GHSP-D-16-00395.

[14] A. N. Doss, D. Shah, G. F. Smaisim, M. Olha, and S. Jaiswal, "A comprehensive analysis of internet of things (IoT) in enhancing data security for better system integrity - a critical analysis on the security attacks and relevant countermeasures," *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022*, Greater Noida, India, 2022, pp. 165–167, doi: 10.1109/ICACITE53722.2022.9823817.

[15] X. Jing, Z. Yan, and W. Pedrycz, "Security data collection and data analytics in the internet: a survey," IEEE Communications Surveys and Tutorials, vol. 21, no. 1, pp. 586–618, Jan. 2019, doi: 10.1109/COMST.2018.2863942.

[16] A. Razaque *et al.*, "Survey: cybersecurity vulnerabilities, attacks and solutions in the medical domain," *IEEE Access*, vol. 7, pp. 168774–168797, 2019, doi: 10.1109/ACCESS.2019.2950849.

[17] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, "Detecting cybersecurity attacks across different network features and learners," *Journal of Big Data*, vol. 8, no. 38, pp. 1-29, Dec. 2021, doi: 10.1186/s40537-021-00426-w.

[18] A. Sharma and H. Babbar, "Evaluation and analysis: internet of things using machine learning algorithms for detection of DDoS attacks," *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Bengaluru, India, 2023, pp. 1203-1208, doi: 10.1109/IITCEE57236.2023.10090917.

[19] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[20] O. Ben Fredj, A. Mihoub, M. Krichen, O. Cheikhrouhou, and A. Derhab, "Cybersecurity attack prediction: a deep learning approach," in Proceedings of the 13th International Conference on Security of Information and Networks, Merkez, Turkey, Nov. 2020, pp. 1–6, doi: 10.1145/3433174.3433614.

[21] A. Mousa, M. Karabatak and T. Mustafa, "Database security threats and challenges," *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116436.

[22] A. Panwar and V. Bhatnagar, "Distributed ledger technology (DLT): the beginning of a technological revolution for blockchain," *2nd International Conference on Data, Engineering and Applications (IDEA)*, Bhopal, India, 2020, pp. 1-5, doi: 10.1109/IDEA49133.2020.9170699.

[23] D. Li, W. E. Wong and J. Guo, "A survey on blockchain for enterprise using hyperledger fabric and composer," *2019 6th International Conference on Dependable Systems and Their Applications (DSA)*, Harbin, China, 2020, pp. 71-80, doi: 10.1109/DSA.2019.00017.

[24] N. Farhadighalati, L. A. Estrada-Jimenez, S. Nikghadam-Hojjati and J. Barata, "A systematic review of access control models: background, existing research, and challenges," in *IEEE Access*, vol. 13, pp. 17777-17806, 2025, doi: 10.1109/ACCESS.2025.3533145.

[25] A. Punia, P. Gulia, N. S. Gill, E. Ibeke, C. Iwendi, and P. K. Shukla, "A systematic review on blockchain-based access control systems in cloud environment," *Journal of Cloud Computing*, vol. 13, art. no. 146, Dec. 2024, doi: 10.1186/s13677-024-00697-7.

[26] S. Lawal and R. Krishnan, "Attribute-based access control policy review in permissioned blockchain," in *Secure Knowledge Management in The Artificial Intelligence Era (SKM 2021)*, San Antonio, TX, USA, Oct. 2021, pp. 97–109, doi: 10.1007/978-3-030-97532-6_6.

[27] S. Ahmadjee, C. Mera-Gómez, R. Bahsoon, and R. Buyya, "Security architectural approaches and risk assessment methods for blockchain systems: a review and future directions," *Distributed Ledger Technologies: Research and Practice*, vol. 5, no. 1, pp. 1–21, Mar. 2026, doi: 10.1145/3721140.

[28] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: vulnerabilities, attacks, and defenses," *ACM Computing Surveys*, vol. 53, no. 3, pp. 1–43, May 2020, doi: 10.1145/3391195.

[29] A. Laurent, L. Brotcorne, and B. Fortz, "Transaction fees optimization in the ethereum blockchain," *Blockchain: Research and Applications*, vol. 3, no. 3, p. 100074, Sep. 2022, doi: 10.1016/j.bcra.2022.100074.

[30] A. Alghuried, M. Alkinoon, M. Mohaisen, A. Wang, C. C. Zou, and D. Mohaisen, "Blockchain security and privacy: threats, challenges, applications, and tools," distributed ledger technologies: research and practice, vol. 5, no. 1, pp. 1–61, Feb. 2025, doi: 10.1145/3716323.

[31] S. Martinez, A. Ameigenda, B. De Barros, G. Llambias, L. González, and R. Ruggia, "Leveraging zero-knowledge proofs for blockchain interoperability: experiences with ethereum and hyperledger fabric," in *Proceedings of the 2024 L Latin American Computer Conference (CLEI)*, Buenos Aires, Argentina, Aug. 2024, pp. 1–10, doi: 10.1109/CLEI64178.2024.10700385.

[32] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie and X. Peng, "A survey on zero-knowledge proof in blockchain," in *IEEE Network*, vol. 35, no. 4, pp. 198-205, Jul./Aug. 2021, doi: 10.1109/MNET.011.2000473.

[33] A. Diro, L. Zhou, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, Feb. 2024, doi: 10.1016/j.jisa.2023.103678.

[34] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ Publishing Group*, vol. 372, no. 71, pp. 10-9, Mar. 2021, doi: 10.1136/bmj.n71.

[35] A. Mathur, A. Dabas and N. Sharma, "Evolution from industry 1.0 to industry 5.0," *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, 2022, pp. 1390-1394, doi: 10.1109/ICAC3N56670.2022.10074274.

[36] K. Tantawi, I. Fidan, O. Huseynov, Y. Musa, and A. Tantawy, "Advances in industry 4.0: from intelligentization to the industrial metaverse," *International Journal on Interactive Design and Manufacturing*, vol. 19, pp. 1461–1472, Mar. 2025, doi: 10.1007/s12008-024-01750-0.

[37] A. P. Saha and U. Guin, "Optimizing supply chain management using permissioned blockchains," in *ICCAD '24: 43rd IEEE/ACM International Conference on Computer-Aided Design*, New York, NY, USA: Association for Computing Machinery, Apr. 2025, pp. 1–7. doi: 10.1145/3676536.3689918.

[38] M. M. H. Onik, M. H. Miraz, and C.-S. Kim, "A recruitment and human resource management technique using blockchain technology for industry 4.0," in *Smart Cities Symposium 2018*, Bahrain, 2018, pp. 1–6. doi: 10.1049/cp.2018.1371.

[39] A. N. Mohammad Saif and M. A. Islam, "Blockchain in human resource management: a systematic review and bibliometric analysis," *Technology Analysis & Strategic Management*, vol. 36, no. 4, pp. 635–650, Mar. 2024, doi: 10.1080/09537325.2022.2049226.

[40] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-id: a blockchain-based decentralized identity management for remote healthcare," Healthcare, vol. 9, no. 6, p. 712, Jun. 2021, doi: 10.3390/healthcare9060712.

[41] X. Li, J. Luo, L. Zhou, and H. Wang, "A blockchain-based personal health record sharing scheme with security and privacy preservation," in *Information Security and Cryptology*, M. Ge Chunpeng and Yung, Ed., Singapore: Springer Nature Singapore, 2024, pp. 141–159. doi: 10.1007/978-981-97-0942-7_8.

[42] V. Keršič and M. Turkanović, "A review on building blocks of decentralized artificial intelligence," *ICT Express*, vol. 11, no. 3, pp. 486–506, Jun. 2025, doi: 10.1016/j.icte.2025.04.001.

[43] H. M. N. D. Bandara, M. Staples, and S. Malik, "Designing for shared ledgers in industry ecosystems," *Distributed Ledger Technologies: Research and Practice*, vol. 5, no. 3, pp. 1-27, Sep. 2026, doi: 10.1145/3724410.

[44] R. Soltani, U. T. Nguyen, and A. An, "Distributed ledger technologies and their applications," *Applied Sciences*, vol. 12, no. 15, p. 7898, Aug. 2022, doi: 10.3390/app12157898.

[45] T. L. Nguyen *et al.*, "Blockchain-empowered trustworthy data sharing: fundamentals, applications, and challenges," *ACM Computing Surveys*, vol. 57, no. 8, pp. 1–36, Mar. 2025, doi: 10.1145/3718082.

[46] D. Ravi, S. Ramachandran, R. Vignesh, V. R. Falmari, and M. Brindha, "Privacy preserving transparent supply chain management through hyperledger fabric," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100072, Jun. 2022, doi: 10.1016/J.BCRA.2022.100072.

[47] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system." Accessed: May 18, 2025. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[48] Y. Ucbas, A. Eleyan, M. Hammoudeh, and M. Alohaly, "Performance and Scalability analysis of ethereum and hyperledger fabric," *IEEE Access*, vol. 11, pp. 67156–67167, Jul. 2023, doi: 10.1109/ACCESS.2023.3291618.

[49] I. Yousaf, A. Abrar, and L. Yarovaya, "Decentralized and centralized exchanges: Which digital tokens pose a greater contagion risk?," *Journal of International Financial Markets, Institutions and Money*, vol. 89, , p. 101881, Dec. 2023, doi: 10.1016/j.intfin.2023.101881.

[50] W. Deng, T. Huang, and H. Wang, "A review of the key technology in a blockchain building decentralized trust platform," *Mathematics*, vol. 11, no. 1, p. 101, Dec. 2023, doi: 10.3390/math11010101.

[51] L. Chen, J. Zhu, Y. Xu, H. Zheng, and S. Su, "A framework based on the DAO and NFT in blockchain for electronic document sharing," *CMES - Computer Modeling in Engineering and Sciences*, vol. 140, no. 3, pp. 2373–2395, Jul. 2024, doi: 10.32604/cmes.2024.049996.

[52] M. Xu *et al.*, "Exploring blockchain technology through a modular lens: a survey," *ACM Computing Surveys*, vol. 56, no. 9, pp. 1–39, Oct. 2024, doi: 10.1145/3657288.

[53] Adarsh and H. Kaur, "Decentralized social media based on ethereum blockchain and IPFS," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, New York, NY, USA, Dec. 2024, pp. 112–116. doi: 10.1145/3678610.3678624.

[54] B. L. Y. Quan, N. H. A. Wahab, J. N. Fadila, Y. Aun, S. K. L. Luk, and K. Y. Wong, "The frontier of blockchain privacy: development of a private ethereum network," in *14th IEEE Symposium on Computer Applications and Industrial Electronics, ISCAIE 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 117–122. doi: 10.1109/ISCAIE61308.2024.10576280.

[55] T. Jiao, Z. Xu, M. Qi, S. Wen, Y. Xiang, and G. Nan, "A survey of ethereum smart contract security: attacks and detection," *Distributed Ledger Technologies: Research and Practice*, vol. 3, no. 3, pp. 1–28, Sep. 2024, doi: 10.1145/3643895.

[56] H. Li *et al.*, "FISCO-BCOS: an enterprise-grade permissioned blockchain system with high-performance," in *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, Denver, CO, USA, Nov. 2023, art. no. 68, pp. 1–17, doi: 10.1145/3581784.3607053.

[57] S. Arsheen and K. Ahmad, "Immunechain: a blockchain-based secure and transparent vaccine supply chain," *SN Computer Science*, vol. 6, no. 1, p. 40, Dec. 2024, doi: 10.1007/s42979-024-03421-z.

[58] S. Ben Othman and M. Getahun, "Leveraging blockchain and IoMT for secure and interoperable electronic health records," *Scientific Reports*, vol. 15, no. 1, p. 12358, Dec. 2025, doi: 10.1038/s41598-025-95531-8.

[59] E. Psarra, D. Apostolou, Y. Verginadis, I. Patiniotakis, and G. Mentzas, "Permissioned blockchain network for proactive access control to electronic health records," *BMC Medical Informatics Decision Making*, vol. 24, no. 1, p. 303, Dec. 2024, doi: 10.1186/s12911-024-02708-8.

[60] L. Wu, W. Lu, L. Chu, and C. Chen, "Visualizing blockchain in construction projects: status quo, challenges, and a guideline for implementation," *Frontiers of Engineering Management*, vol 12, no. 3, pp. 467–486, Jul. 2025, doi: 10.1007/s42524-024-4034-6.

[61] R. Kumar, S. S. Patil, A. S. Patil, A. B. Patil, and S. B. Patil, "Courtsafe: legal records storage & management using blockchain," in *Proceedings of the 16th International Conference on Contemporary Computing*, Noida, India, Oct. 2024, pp. 227–232, doi: 10.1145/3675888.3676140.

[62] I. Surjandari, H. Yusuf, E. Laoh, and R. Maulida, "Designing a permissioned blockchain network for the halal industry using hyperledger fabric with multiple channels and the raft consensus mechanism," *Journal of Big Data*, vol. 8, no. 10, pp.1-16, Dec. 2021, doi: 10.1186/s40537-020-00405-7.

[63] A. Noorain, K. Ahmad, and L. E. M. Ricci, "Private and consortium blockchain," in *Fostering Machine Learning and IoT for Blockchain Technology: Smart Cities Applications, Volume 1*, K. Ahmad, U. N. Dulhare, M. S. Badar, J. Ahamed, and M. A. Rizvi, Eds. Singapore: Springer, 2025, pp. 189–213. doi: 10.1007/978-981-96-4078-2_6.

[64] B. Liu, H. Tian, Z. Shen, Y. Xu, and W. Dou, "A consortium blockchain-based edge task offloading method for connected autonomous vehicles," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 20, no. 3, p. 19, Sep. 2025, doi: 10.1145/3696004.

[65] K. Sha, K.-B. Yue, W. Wei, Y. Wu, M. Koduru, and P. Vuchuru, "Consortiumsec: blockchain-based distributed security framework for consortium applications," *Distributed Ledger Technologies: Research and Practice*, vol. 4, no. 4, pp. 1– 19, Dec. 2025, doi: 10.1145/3699965.

[66] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: a comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, Jun. 2021, doi: 10.1016/j.icte.2020.09.002.

[67] M. A. Manolache, S. Manolache, and N. Tapus, "Decision making using the blockchain proof of authority consensus," in *Procedia Computer Science*, vol. 199, pp. 580–588, Feb. 2022, doi: 10.1016/j.procs.2022.01.071.

[68] V. Jayadev, N. Moradpoor, and A. Petrovski, "Assessing the performance of ethereum and hyperledger fabric under DDoS attacks for cyber-physical systems," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, Vienna, Austria, Jul.–Aug. 2024, art. no. 48, pp. 1–6, doi: 10.1145/3664476.3670927.

[69] D. Hawashin *et al.*, "Leveraging hyperledger fabric for enhanced compliance monitoring in UAV operations," *Distributed Ledger Technologies: Research and Practice*, vol. 5, no. 1, p. 3, Mar. 2026, doi: 10.1145/3716324.

[70] M. Rifat Hossain, F. A. Nirob, A. Islam, T. M. Rakin, and M. Al-Amin, "A comprehensive analysis of blockchain technology and consensus protocols across multilayered framework," *IEEE Access*, vol. 12, pp. 63087–63129, Apr. 2024, doi: 10.1109/ACCESS.2024.3395536.

[71] S. N. Pari, S. Rajashree, A. Prakash and R. M. Shanthosh, "Role based access control framework for healthcare records using hyperledger fabric," *2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Ghaziabad, India, 2022, pp. 1-7, doi: 10.1109/ICICT55121.2022.10064512.

[72] L. Olivieri, L. Negrini, V. Arceri, P. Ferrara, and A. Cortesi, "Detection of read-write issues in hyperledger fabric smart contracts," in *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing*, New York, NY, USA: ACM, Mar. 2025, pp. 329–337. doi: 10.1145/3672608.3707721.

[73] H. Liu, D. Han, and D. Li, "Fabric-iot: A blockchain-based access control system in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, Jan. 2020, doi: 10.1109/ACCESS.2020.2968492.

[74] N. M. S. Al-Gburi, A. Földvári, K. Marussy, O. Semeráth, and I. Kocsis, "Requirement-driven generation of distributed ledger architectures," in *Proceedings of the ACM/IEEE 27th International Conference on Model Driven Engineering Languages and Systems*, Linz, Austria, Sep. 2024, pp. 772–782, doi: 10.1145/3640310.3674097.

[75] A. Barger, V. Gorgadze, and A. Sanina, "Enhancing state integrity and validation in hyperledger fabric with certification blocks and patricia merkle tries," in *Proceedings of the 2024 7th International Conference on Blockchain Technology and Applications*, Xi'an, China, Dec. 2024, pp. 11–18, doi: 10.1145/3708622.3708624.

[76] G. Al-Sumaidaee, R. Alkhudary, Z. Zilic, and A. Swidan, "Performance analysis of a private blockchain network built on hyperledger fabric for healthcare," *Information Processing Management*, vol. 60, no. 2, p. 103160, Mar. 2023, doi: 10.1016/j.ipm.2022.103160.

[77] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proceedings of the 2014 USENIX Annual Technical Conference*, Philadelphia, PA, USA, Jun. 2014, pp. 305–319, doi: 10.5555/2643634.2643666.

[78] R. Dautov and E. J. Husom, "Raft protocol for fault tolerance and self-recovery in federated learning," in *Proceedings - 2024 IEEE/ACM 19th Symposium on Software Engineering for Adaptive and Self-Managing Systems, SEAMS 2024*, Lisbon AA, Portugal, Apr. 2024, pp. 110–121. doi: 10.1145/3643915.3644093.

[79] Y. Liu *et al.*, "Fully anonymous decentralized identity supporting threshold traceability with practical blockchain," in *Proceedings of the ACM on Web Conference 2025*, New York, NY, USA: ACM, Apr. 2025, pp. 3628–3638. doi: 10.1145/3696410.3714762.

[80] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, "Pricollabanalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation," *Cluster Computing*, vol. 28, no. 3, p. 191, Jun. 2025, doi: 10.1007/s10586-024-04928-z.

[81] R. K. Kaushal, N. Kumar, V. Kukreja, and E. Boonchieng, "Hyperledger fabric based remote patient monitoring solution and performance evaluation," *Peer-to-Peer Networking and Applications*, vol. 18, no. 3, p. 105, Jun. 2025, doi: 10.1007/s12083-025-01921-0.

[82] M. S. Farooq *et al.*, "Client engagement solution for post implementation issues in software industry using blockchain," *Scientific Reports*, vol. 15, no. 1, p. 11806, Dec. 2025, doi: 10.1038/s41598-025-95448-2.

[83] G. Kumar, R. Saha, M. Conti, and T. H. Kim, "DEBPIR: enhancing information privacy in decentralized business modeling," *Complex & Intelligent Systems*, vol. 11, no. 7, p. 290, Jul. 2025, doi: 10.1007/s40747-025-01868-y.

[84] S. Babu Erukala, D. Tokmakov, A. Devi Aguru, R. Kaluri, A. Bekyarova-Tokmakova and N. Mileva, "An end-to-end secure communication framework for smart homes environment using consortium blockchain system," in *IEEE Access*, vol. 13, pp. 67250-67268, Apr. 2025, doi: 10.1109/ACCESS.2025.3559070.

[85] M. Abdullah Al Mamun, M. Li, B. Kumar Pramanik, F. Hussain and A. Z. M. Shakilur Rahman, "Leveraging blockchain technology with enhanced MDSVA for robust meteorological sensor data validation," in *IEEE Access*, vol. 13, pp. 72633-72656, Apr. 2025, doi: 10.1109/ACCESS.2025.3563099.

[86] S. Wang, N. Luo, B. Xing, Z. Sun, H. Zhang, and C. Sun, "Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products," *Scientific Reports*, vol. 14, no. 1, p. 20048, Aug. 2024, doi: 10.1038/s41598-024-70533-0.

[87] A. Tepelidis, E. E. Mitsopoulou, A. T. Patenidis, K. Livitckaia, K. Votis, and D. Tzovaras, "Blockademic: a digital distributed verification system for educational activities in higher education," *Distributed Ledger Technologies: Research and Practice*, vol. 4, no. 3, p. 20, Sep. 2025, doi: 10.1145/3703463.

[88] A. De Salve, D. Di Francesco Maesa, P. Mori, L. Ricci, and A. Puccia, "A multi-layer trust framework for self sovereign identity on blockchain," *Online Social Networks and Media*, vol. 37–38, p. 100265, Sep. 2023, doi: 10.1016/j.osnem.2023.100265.

[89] C. D. N. Kyriakidou, I. Pittaras, A. M. Papathanasiou, G. Xylomenos, and G. C. Polyzos, "Performance of smart contract-based digital twins for the internet of things," in *Proceedings of the 2nd ACM International Workshop on Middleware for Digital Twins*, Hong Kong, China, Dec. 2024, pp. 1–6, doi: 10.1145/3702636.3703442

[90] A. Pisu, L. Pompianu, S. Castello, D. Riboni, and S. Carta, "Sustainable certification of local communities data through smart contracts," in *Proceedings of the 2024 International Conference on Information Technology for Social Good*, Bremen, Germany, Sep. 2024, pp. 420–428, doi: 10.1145/3677525.3678692.

[91] S. Sai, V. Chamola, K. -K. R. Choo, B. Sikdar and J. J. P. C. Rodrigues, "Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: a review," in *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5873-5897, Apr. 2023, doi: 10.1109/JIOT.2022.3232793.

[92] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based distributed application for multimedia system using hyperledger fabric," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 2473–2499, Jan. 2024, doi: 10.1007/s11042-023-15690-6.

[93] F. Kirstein, A. Altenbernd, S. Schimmler, and M. Hauswirth, "A decentralised persistent identification layer for DCAT datasets," in *ACM Web Conference 2023 - Companion of the World Wide Web Conference, WWW 2023*, Austin, TX, USA, Apr. 2023, pp. 1424–1427. doi: 10.1145/3543873.3587589.

[94] A. Tahar, G. Mendy, and S. Ouya, "Implementing multisignature on a blockchain-based land administration system: securing land rights and enhancing transparency," in *ACM International Conference Proceeding Series*, Osaka, Japan, Jul. 2023, pp. 8–14. doi: 10.1145/3625078.3625080.

[95] V. Bonnici *et al.*, "BIOCHAIN: towards a platform for securely sharing microbiological data," in *ACM International Conference Proceeding Series*, Heraklion, Crete, Greece, May 2023, pp. 59–63. doi: 10.1145/3589462.3589501.

[96] I. P. Chochliouros *et al.*, "NEMO: building the next generation meta operating system," in *Proceedings of the 3rd Eclipse Security, AI, Architecture and Modelling Conference on Cloud to Edge Continuum (eSAAM '23)*, Ludwigsburg, Germany, Oct. 2023, pp. 1–9. doi: 10.1145/3624486.3624504.

[97] S. Mohan M and L. Sujihelen, "An efficient chain code for access control in hyper ledger fabric healthcare system," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 5, p. 100204, Sep. 2023, doi: 10.1016/j.prime.2023.100204.

[98] Hyperledger Fabric, *Hyperledger Fabric Documentation*. Accessed: May. 22, 2026 [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/index.html.

[99] IBM, "Hyperledger Fabric reference," *IBM Documentation*, ver. 2.5.4. Accessed: May. 22, 2026 [Online]. Available: https://www.ibm.com/docs/en/blockchain-platform/2.5.4?topic=reference-hyperledger-fabric.

[100] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*. USA: Artech House, Inc., 2003.

[101] A. De Salve, L. Franceschi, A. Lisi, P. Mori, and L. Ricci, "L2DART: a trust management system integrating blockchain and off-chain computation," *ACM Transactions on Internet Technology*, vol. 23, no. 1, pp. 1–30, Feb. 2023, doi: 10.1145/3561386.

[102] E. Sivakumar, K. J. Singh, P. Chawla and G. Ganesan, "RBEDH: a decentralized role-based event driven hybrid framework for smart contracts," in *IEEE Access*, vol. 13, pp. 74781-74798, Mar. 2025, doi: 10.1109/ACCESS.2025.3554630.

[103] C. Daah, A. Qureshi, I. Awan, and S. Konur, "Simulation-based evaluation of advanced threat detection and response in financial industry networks using zero trust and blockchain technology," *Simulation Modelling Practice and Theory*, vol. 138, p. 103027, Jan. 2025, doi: 10.1016/j.simpat.2024.103027.

[104] T. Zaidi, M. Usman, M. U. Aftab, H. Aljuaid, and Y. Y. Ghadi, "Fabrication of flexible role-based access control based on blockchain for internet of things use cases," *IEEE Access*, vol. 11, pp. 106315–106333, Sep. 2023, doi: 10.1109/ACCESS.2023.3318487.

[105] S. Sutradhar, S. Karforma, R. Bose, S. Roy, S. Djebali, and D. Bhattacharyya, "Enhancing identity and access management using hyperledger fabric and OAUth 2.0: A block-chain-based approach for security and scalability for healthcare industry," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 49–67, Jan. 2024, doi: 10.1016/j.iotcps.2023.07.004.

[106] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, Dec. 2016, doi: 10.1002/sec.1748.

[107] P. Ruan, Y. Kanza, B. C. Ooi, and D. Srivastava, "Ledgerview: access-control views on hyperledger fabric," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, Philadelphia, PA, USA, Jun. 2022, pp. 2218–2231. doi: 10.1145/3514221.3526046.

[108] I. Makhdoom, M. Abolhasan, J. Lipman, M. Piccardi, and D. Franklin, "Privysec: a secure and privacy-compliant distributed framework for personal data sharing in IoT ecosystems," *Blockchain: Research and Applications*, vol. 5, no. 4, p. 100220, Dec. 2024, doi: 10.1016/j.bcra.2024.100220.

[109] A. Singh, S. Sural, T. Sengupta, and S. Sural, "Avchain: trusted sharing of autonomous vehicle crash incident data using interoperating hyperledger fabric networks and IPFS," *Distributed Ledger Technologies: Research and Practice*, vol. 5, no. 3, pp. 1–29, Dec. 2025, doi: 10.1145/3709158.

[110] A. K. Peepliwal *et al.*, "A prototype model of zero trust architecture blockchain with eigentrust-based practical byzantine fault tolerance protocol to manage decentralized clinical trials," *Blockchain: Research and Applications*, vol. 5, no. 4, p. 100232, Dec. 2024, doi: 10.1016/j.bcra.2024.100232.

[111] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "Accesschain: An access control framework to protect data access in blockchain enabled supply chain," *Future Generation Computer Systems*, vol. 148, pp. 380–394, Nov. 2023, doi: 10.1016/j.future.2023.06.009.

[112] G. Dalabanjan and D. G. Narayan, "Enabling attribute-based access control for openstack cloud resources through smart contracts," in *Procedia Computer Science*, vol. 233, pp. 861–871, Apr. 2024, doi: 10.1016/j.procs.2024.03.275.

[113] U. Roy and N. Ghosh, "Bloac: a blockchain-based secure access control management for the internet of things," Journal of Information Security and Applications, vol. 87, p. 103897, Dec. 2024, doi: 10.1016/j.jisa.2024.103897.

[114] N. Wu, L. Xu, and L. Zhu, "A blockchain based access control scheme with hidden policy and attribute," *Future Generation Computer Systems*, vol. 141, pp. 186–196, Apr. 2023, doi: 10.1016/j.future.2022.11.006.

[115] G. Madkaikar, K. S. M. Yelisetty, S. Sural, J. Vaidya, and V. Atluri, "Performance analysis of dynamic ABAC systems using a queuing theoretic framework," *Computers & Security*, vol. 154, p. 104432, Jul. 2025, doi: 10.1016/j.cose.2025.104432.

[116] M. Li, J. Xue, Z. Liu, Y. Suo, T. Lei, and Y. Wang, "DAMFSD: A decentralized authorization model with flexible and secure delegation," *Internet of Things*, vol. 27, p. 101317, Oct. 2024, doi: 10.1016/j.iot.2024.101317.

[117] C. Doulkeridis, I. Chrysakis, S. Karagiorgou, P. Kranas, G. Makridis, and Y. Theodoridis, "The mobispaces manifesto on mobility data spaces," in *Proceedings of the 4th Eclipse Security, AI, Architecture and Modelling Conference on Data Space (eSAAM '24)*, Mainz, Germany, Oct. 2024, pp. 66–75. doi: 10.1145/3685651.3685654.

[118] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "TABI: trust-based abac mechanism for edge-iot using blockchain technology," *IEEE Access*, vol. 11, pp. 36379–36398, Apr. 2023, doi: 10.1109/ACCESS.2023.3265349.

[119] O. Cheikhrouhou, K. Mershad, M. Laurent, and A. Koubaa, "Blockchain and emerging technologies for next generation secure healthcare: a comprehensive survey of applications, challenges, and future directions," *Blockchain: Research and Applications*, vol. 6, no. 5, art. no. 100305, May 2025, doi: 10.1016/j.bcra.2025.100305.

[120] L. Fotia, F. Delicato, and G. Fortino, "Trust in edge-based internet of things architectures: state of the art and research challenges," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–34, Jan. 2023, doi: 10.1145/3558779.

[121] V. R. Kebande and A. I. Awad, "Industrial internet of things ecosystems security and digital forensics: achievements, open challenges, and future directions," *ACM Computing Surveys*, vol. 56, no. 5, pp. 1–37, May 2024, doi: 10.1145/3635030.

[122] G. Falazi, U. Breitenbucher, F. Leymann, and S. Schulte, "Cross-chain smart contract invocations: a systematic multi-vocal literature review," *ACM Computing Surveys*, vol. 56, no. 6, pp. 1–38, Jan. 2024, doi: 10.1145/3638045.

[123] M. Raikwar, "A review on privacy in DAG-based DLTs," in *Proceedings of the 2024 6th Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS)*, Berlin, Germany, Oct. 2024, pp. 211–214, doi: 10.1109/BRAINS63514.2024.10765357.

[124] X. Liu, H. Liu, X. Liang, and Y. Yao, "A blockchain-based anonymous and regulated e-taxing protocol for art trading," *Digital Communications and Networks*, vol. 11, no. 3, pp. 681–688, Jul. 2025, doi: 10.1016/j.dcan.2025.01.002.

[125] S. Hu, M. Schmidt-Kraepelin, S. Thiebes, and A. Sunyaev, "Mapping distributed ledger technology characteristics to use cases in healthcare: a structured literature review," *ACM Transactions on Computing for Healthcare*, vol. 5, no. 3, pp. 1–33, Jul. 2024, doi: 10.1145/3653076.

[126] P. Zhang, S. Ding, and Q. Zhao, "Exploiting blockchain to make AI trustworthy: a software development lifecycle view," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1–31, Apr. 2024, doi: 10.1145/3614424.

[127] M. J. Alam, I. Hossain, S. Puppala, and S. Talukder, "Combating identity attacks in online social networks: a multi-layered framework using zero-knowledge proof and permissioned blockchain," in *Proceedings of the 2023 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Kusadasi, Turkey, Nov. 2023, pp. 636–643, doi: 10.1145/3625007.3627722.

[128] S. Park *et al.*, "Beyond the blockchain address: zero-knowledge address abstraction," in *Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing*, New York, NY, USA: ACM, Mar. 2025, pp. 366–374. doi: 10.1145/3672608.3707839.

[129] B. Oude Roelink, M. El-Hajj, and D. Sarmah, "Systematic review: comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication," *Security and Privacy*, vol. 7, no. 5, p. e401, Sep. 2024, doi: 10.1002/spy2.401.

[130] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct non-interactive zero knowledge for a von Neumann architecture," in *Proceedings of the 23rd USENIX Security Symposium*, San Diego, CA, USA, Aug. 2014, pp. 781–796, doi: 10.5555/2671225.2671275.

[131] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Fast Reed-Solomon interactive oracle proofs of proximity," in *Proceedings of the 45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, Prague, Czech Republic, Jul. 2018, vol. 107, Art. no. 14, pp. 1–17, Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi: 10.4230/LIPIcs.ICALP.2018.14.

[132] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, Washington, DC, USA, Nov. 2002, pp. 21–30. doi: 10.1145/586110.586114.

[133] T. Wang, Z. Lin, S. Zhang, L. Shi, Q. Yang, and B. Düdder, "Linking souls to humans: blockchain accounts with credible anonymity for web 3.0 decentralized identity," in *WWW 2025 - Proceedings of the ACM Web Conference*, Sydney, NSW, Australia, Apr. 2025, pp. 2668–2676. doi: 10.1145/3696410.3714784.

[134] Y. Zhao *et al.*, "A logarithmic size revocable linkable ring signature for privacy-preserving blockchain transactions," *High-Confidence Computing*, vol. 5, no. 4, p. 100319, Mar. 2025, doi: 10.1016/j.hcc.2025.100319.

[135] V. Keršič, S. Karakatič, and M. Turkanović, "On-chain zero-knowledge machine learning: an overview and comparison," *King Saud bin Abdulaziz University*, vol. 36, no. 9, p. 102207, Nov. 2024, doi: 10.1016/j.jksuci.2024.102207.

[136] J. W. Heo, G. Ramachandran, and R. Jurdak, "nPPoS: non-interactive practical proof-of-storage for blockchain," *Blockchain: Research and Applications*, vol. 5, no. 4, p. 100221, Dec. 2024, doi: 10.1016/j.bcra.2024.100221.

[137] D. J, S. K, K. Singh, and M. S. S, "A privacy-preserving framework for endorsement process in hyperledger fabric," *Computers & Security*, vol. 116, p. 102637, May 2022, doi: 10.1016/j.cose.2022.102637.

[138] B. Nour, H. Khelifi, R. Hussain, S. Mastorakis, and H. Moungla, "Access control mechanisms in named data networks," *ACM Comput. Surv.*, vol. 54, no. 3, pp. 1–35, Jun. 2021, doi: 10.1145/3442150.

[139] S. A. Chaudhry, A. Irshad, K. Yahya, N. Kumar, M. Alazab, and Y. Bin Zikria, "Rotating behind privacy: an improved lightweight authentication scheme for cloud-based IoT environment," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–19, Aug. 2021, doi: 10.1145/3425707.

[140] S. Atiewi *et al.*, "Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography," *IEEE Access*, vol. 8, pp. 113498–113511, Feb. 2020, doi: 10.1109/ACCESS.2020.3002815.

[141] Di. Wang, P. Wang, and C. Wang, "Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 3, pp. 1–26, May 2020, doi: 10.1145/3325130.

[142] Z. Ghaffar, S. Ahmed, K. Mahmood, S. H. Islam, M. M. Hassan, and G. Fortino, "An improved authentication scheme for remote data access and sharing over cloud storage in cyber-physical-social-systems," *IEEE Access*, vol. 8, pp. 47144–47160, Feb. 2020, doi: 10.1109/ACCESS.2020.2977264.

[143] D. Benarroch, M. Campanelli, D. Fiore, K. Gurkan, and D. Kolonelos, "Zero-knowledge proofs for set membership: efficient, succinct, modular," *Designs, Codes and Cryptography*, vol. 91, no. 11, pp. 3457–3525, Nov. 2023, doi: 10.1007/s10623-023-01245-1.

[144] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: past, present, and future trends," *ACM Computing Surveys*, vol. 54, no. 8, pp. 1–41, Oct. 2022, doi: 10.1145/3471140.

[145] Z. Guan, Z. Wan, Y. Yang, Y. Zhou, and B. Huang, "Blockmaze: an efficient privacy-preserving account-model blockchain based on zk-SNARKs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 1446–1463, May-Jun. 2022, doi: 10.1109/TDSC.2020.3025129.