BLOCKCHAIN-BASED INTER-ORGANIZATIONAL INFORMATION SHARING WITH CONFIDENTIALITY PROTECTION: A SYSTEMATIC LITERATURE REVIEW

Mohd Rizal Kadis[1], Saaidal Razalli Azzuhri[1], Miss Laiha Mat Kiah[1], and Tutut Herawan[1]*

[1]Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia

Emails: rizalkadis@gmail.com[1], saaidal@um.edu.my[1*] (Corresponding author), misslaiha@um.edu.my[1], tutut@um.edu.my[1]

ABSTRACT

Blockchain technology has emerged as a transformative solution for inter-organizational information sharing, offering enhanced security and transparency. Transparency aims to build trust, ensure data integrity, guarantee accountability, and prevent unfair practices. However, this presents a dilemma for organizations prioritizing confidentiality, making the full implementation of blockchain challenging. To address these concerns, numerous studies have explored methods for preserving confidentiality and privacy within blockchain systems. Recent research has conducted systematic reviews focusing on security and user-centric approaches to data privacy in blockchain. In this paper, we present a systematic literature review to examine techniques proposed for preserving confidentiality in inter-organizational information sharing. In total, 51 study papers were selected for synthesis. The results indicate the techniques can be categorized into seven groups: privacy-preserving, authorization, data perturbation, symmetric encryption, asymmetric encryption, isolated area, and comprehensive tool. We identified that these techniques are applicable to 11 scenarios, as outlined in this paper.

Keywords: Blockchain; Confidentiality Protection; Inter-organizational Information Sharing; Systematic Literature Review.

1.0 INTRODUCTION

Reciprocal information sharing is pivotal in fostering and sustaining a synergistic environment for delivering exemplary services [1]. Furthermore, information sharing among government agencies increases productivity, performance, operations, improves policy-making, and provides better services to citizens and businesses [2]. For instance, sharing medical information between healthcare institutions, such as hospitals and clinics, allows healthcare professionals to evaluate a patient's medical history, including allergies and prior treatments. This facilitates the delivery of the most effective and timely care, significantly benefiting the healthcare system, particularly in emergencies or when a patient seeks treatment at a different facility. In another scenario, information sharing from stakeholders in the food industry to consumers regarding the food supply chain enables the tracing of the origin of food products. This approach enhances transparency for consumers, particularly for Muslim consumers who prioritize halal food sources and those concerned about food safety. In public services, the sharing of information among government agencies facilitates the rapid implementation of policies in areas such as subsidy distribution to citizens, pension provision, and economic planning, all while minimizing resource costs, including time, manpower, and finances.

However, not all organizations are inclined to share information with others due to various factors, including the sensitivity and intrinsic value of the information, regulatory compliance issues, lack of trust, and concerns over potential information breaches. All these factors are fundamentally tied to a core principle of information security: confidentiality [3]. Confidentiality was identified as one of the six key challenges in inter-organizational information sharing [4]. Consequently, any information-sharing platform must incorporate robust confidentiality measures to address these concerns adequately. In this article, we use the term 'information' to indicate that the data shared by an organization must be a complete set of raw data capable of conveying meaningful value to other organizations.

Blockchain technology has ushered in a paradigm shift in how information sharing is orchestrated, offering a significantly more sophisticated approach in the modern era. Since its introduction by Satoshi Nakamoto [5], blockchain technology, initially developed for cryptocurrency, has gained traction as a reliable and permanent record-keeping solution across various fields. It offers a decentralized digital ledger system that records transactions across multiple computers in a way that ensures data security, transparency, integrity, and high availability. Numerous researchers have explored blockchain as a platform for information sharing across various industries, including healthcare, IoT, automotive, finance, defense, intellectual property, and record management.

The significant advantage of blockchain technology is that it creates immutable transaction records that cannot be edited or deleted. The transaction record is stored in the form of an append-only chain of blocks that are connected to each other in chronological order. Every participating organization in the blockchain network has a copy of these blocks, making it a distributed database. Therefore, blockchain has been recognized as a trusted and secure platform for inter-organizational information sharing.

In the context of safeguarding data confidentiality in inter-organizational information sharing, access to sensitive information should be strictly governed by organizational policies rather than to the individual discretion. Each organization must have the capability to define and enforce which parties are authorized to access and view the data, including other participating organizations within the network. This concept diverges from the user-centric approach extensively researched by numerous scholars [6]–[10], particularly within the healthcare domain, to meet regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR). Drawing from existing literature, this paper seeks to consolidate knowledge on techniques used for safeguarding information confidentiality in blockchain-based inter-organizational information sharing. By understanding these techniques, organizations can better evaluate their needs, select tailored solutions, and enable developers and system architects to incorporate confidentiality-preserving features into blockchain systems. Moreover, this study lays the groundwork for further exploration of untapped information protection methods, fostering deeper and more innovative research in the field. To achieve this, a Systematic Literature Review (SLR) was conducted to provide a comprehensive understanding of the current advancements in blockchain technology for safeguarding data confidentiality in inter-organizational contexts.

This paper makes the following contributions as follows: 1) A systematic literature review on how blockchain facilitates information sharing between organizations, with an emphasis on data confidentiality protection. 2) An analysis of the usage patterns of different blockchain types and data storage strategies. 3) A comprehensive identification of techniques employed alongside blockchain to ensure data confidentiality. 4) A detailed examination of scenarios where these techniques are implemented.

The subsequent sections of the paper are organized as follows: Section 2 provides an overview of blockchain technology and its architectural design. Section 3 deliberates on related works regarding systematic literature reviews of blockchain technology. Section 4 outlines the research methodology used to conduct the systematic literature review. Section 5 presents an analysis of the data extraction results. Section 6 discusses the findings and identifies research gaps for future studies. Finally, Section 7 summarizes the findings and addresses the key questions posed at the beginning of the research.

2.0 OVERVIEW OF BLOCKCHAIN TECHNOLOGY

The design of blockchain architecture is primarily shaped by considerations of scalability and security. From a security perspective, the architectural design is shaped by the intended openness of the stored information, whether it is designated for public access or restricted to internal use only. As a result, blockchain has been developed based on two models: permissionless and permissioned. The permissionless model allows open participation, enabling any user to join the network without prior verification. Conversely, a permissioned model enforces controlled access, permitting only authorized participants to join the network. Meanwhile, the integration of both models into a hybrid architecture enables the combined utilization of functionalities provided by permissioned and permissionless models. A hybrid blockchain achieves a balance between security, privacy, and openness by storing certain information in private networks while allowing other information to remain publicly accessible. In the context of permissioned blockchain, it can be categorized into two distinct types: consortium blockchain and private blockchain. A consortium blockchain is a partially decentralized system where multiple organizations collaboratively manage the network, while a private blockchain is fully centralized, with a single organization maintaining control over the network [11]. Both categories provide tailored solutions depending on the level of decentralization and trust required within the network. Fig. 1 illustrates how each type of blockchain is interconnected.

Nevertheless, blockchain is not a comprehensive standalone solution to replace conventional databases due to ongoing challenges related to privacy and scalability [7], [12]. As blockchain fosters transparency, all organizations within the network can access and view the transactions recorded in the ledger. In other words, once data is stored on the blockchain, every participating organization in the network can view it in plaintext. This situation raises security concerns, particularly related to data confidentiality, which can hinder some organizations from engaging in information sharing. To address these challenges, researchers are actively exploring the integration of blockchain with other techniques, proposing customized blockchain-based models for specific domains. According to Franciscon et al. [13], blockchain architectures can vary depending on the application type and are not restricted to a single model.

In another aspect, blockchain technology emphasizes its core functionality of traceability to enhance trust. However, its limited block capacity restricts the storage of large datasets directly within the blockchain. This limitation arises from the use of propagation mechanisms, as smaller blocks are quicker to validate and propagate across the network, helping to prevent congestion. Larger block sizes increase computational demands during this

process, requiring more time and resources, which can reduce overall efficiency and scalability. It will also consume a high amount of gas, thereby increasing operational costs. Certain blockchain platforms, like Ethereum, impose a gas limit per block, which restricts the inclusion of transactions when the total gas consumed exceeds the block's capacity [14]. Meanwhile, Bitcoin has only a 1MB block size limit. A small block size is not only designed to ensure low latency and high throughput but also results in reduced computational efficiency, limiting the amount of data that can be stored within a single transaction. Consequently, the blockchain's overall capacity to handle large datasets becomes problematic. To address this issue, many researchers have turned to off-chain storage solutions. However, off-chain storage introduces a trade-off in terms of immutability, as data stored off-chain is susceptible to deletion or becoming inaccessible. While solutions like IPFS offer immutability features, they are not entirely risk-free. For instance, when files are stored on a single node without being pinned across multiple nodes, node-level failures or deletions, known as garbage collection, could lead to data loss or unavailability [15].

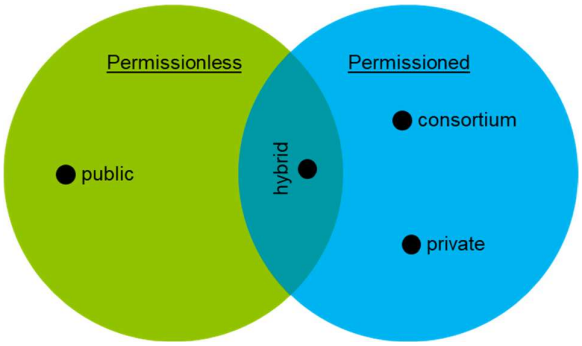

Fig. 1: Blockchain model.

3.0 RELATED WORK

In the past few years, blockchain technology has demonstrated potential applications beyond cryptocurrency, especially in domains centered on information sharing. Numerous studies have reviewed the use of blockchain as a decentralized data storage solution. Table 1 provides an overview of prior reviews on blockchain applications beyond cryptocurrency.

The authors in [16] explored the application of blockchain technology beyond cryptocurrencies, particularly in the context of the Internet of Things (IoT). They found that while blockchain does not guarantee complete anonymity, it supports a partial form of anonymity known as pseudonymity. Pseudonymity is a concept where an individual's identity is concealed using a pseudonym. However, this does not provide full anonymity, as transactions associated with the pseudonym can still be traced through analysis. In terms of security, blockchain can also be leveraged for access permission management or access control using smart contracts. The authors of [19] in their review also focused on the use of blockchain and IoT, particularly in areas related to security and privacy. Their study highlighted that the blockchain trilemma - scalability, security, and decentralization - remains a significant challenge, as these three aspects cannot be achieved simultaneously in a public blockchain and often involve trade-offs among them.

In their review, the authors in [17] emphasized the importance of medical records in healthcare in their review, compiling studies that demonstrate how patient privacy is protected using blockchain technology by adopting a user-centric approach. Meanwhile, the authors in [18] focused on how blockchain manages privacy and anonymization in cybersecurity and personal data management. This review explores blockchain's privacy, anonymization, risks of traceability, and challenges in IoT, GDPR compliance, and secure data handling. Through their study, they found that privacy and anonymization are linked to ensure untraceable user identities.

The authors of [20] conducted an SLR on the application of blockchain in cybersecurity. Their findings revealed that blockchain applications focused on security primarily revolve around areas such as IoT, data sharing, network security, data privacy, and the World Wide Web. The authors of [21] highlighted concerns about the impact of public blockchains on GDPR compliance. Their SLR findings revealed differing opinions on whether blockchain pseudonymization provides sufficient anonymity for GDPR-compliant storage, with no clear consensus on effective techniques.

Most reviews conducted by researchers focus on the potential use of blockchain technology as a medium for information sharing across various fields, including healthcare, IoT, the public sector, and GDPR compliance. These reviews primarily emphasize data privacy protection, often adopting a user-centric approach. Privacy is about the rights and choices of individuals regarding how their personal data is managed and shared. However, to the best of our knowledge, no systematic literature review specifically addresses blockchain-based inter-organizational information sharing with a focus on techniques for ensuring data confidentiality. This paper aims to fill that gap in the existing literature.

Table 1: List of papers conducting systematic literature reviews on blockchain technology

Paper	Keyword	Papers Selected	Sources	Research Questions	Commentary
[16]	"blockchain"	35	IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar	1. What are the use cases of the blockchain beyond cryptocurrencies? 2. Are there any use cases applicable to the IoT? 3. What are the implementation differences with respect to the Bitcoin blockchain? 4. What is the degree of integrity, anonymity and adaptability?	Focus on blockchain-based privacy-by design for IoT
[17]	"Blockchain" AND ("Healthcare" OR "EHR" OR "Medicine" OR "Electronic Health Record")	51	Google Scholar, IEEE Xplore, ACM, Science Direct, Springer, Taylor & Francis, Wiley, Inderscience, Sage, Emerald, Wiley, MDPI, and Hindawi	1. What are the advantages and disadvantages of using Blockchain in Healthcare? 2. How the patient's privacy in EHR is guaranteed by Blockchain? 3. How the patient's security in EHR is guaranteed by Blockchain? 4. What evaluation metrics are applied for evaluating the Blockchain-based approaches for improving security and privacy in healthcare? 5. What are the tools or frameworks used in the Blockchain-based approaches for improving security and privacy in healthcare? 6. What kind of Blockchain was used in the existing research studies? 7. What are the open issues and future research directions of using Blockchain for improving the privacy and security of healthcare?	Focus on the application of blockchain in the healthcare domain.
[18]	"blockchain" and "anonymity" and "privacy" and not "bitcoin"	28	Scopus, Science Direct, IEEE Xplore, Springer, ACM Digital Library, and Google Scholar	1. How does blockchain use anonymity to guarantee privacy? 2. What are the disadvantages of blockchain to adapt to the GDPR? 3. How were the problems encountered addressed? 4. Proposals for future research offered by the publications.	Focus on blockchain privacy through anonymity and GDPR adaptation challenges.

Table 1: Continued

Paper	Keyword	Papers Selected	Sources	Research Questions	Commentary
[19]	((“Blockchain ” OR “Blockchain Technology” OR “BC”) AND (“ Internet of Things “ OR “ IoT”) AND (“Privacy” OR “Security” OR “Confidentiality” OR “Integrity” OR “Availability” OR “Scalability” OR “Authentication & Data Protection” OR “Authorization ” OR “Access Control” OR “Identity Verification”)) .	43	IEEE Explore, ScienceDirect, SpringerLink, ACM Digital Library, MDPI and Wiley.	Not mentioned	Focus on blockchain technology and its applications for enhancing security and privacy in IoT systems
[20]	(“blockchain” OR “block-chain” OR “distributed ledger”) AND (“cyber security” OR “cybersecurity ” OR “cyber-security”)	42	IEEE Xplore, ScienceDirect, SpringerLink, CM Digital Library and Google Scholar	1. What are the latest blockchain applications focused on security? 2. How is blockchain used to improve cyber security? 3. What methods are available for blockchain solutions to manage security without requiring a cryptocurrency token?	Focus on blockchain applications that enhance cybersecurity
[21]	((blockchain* OR Bitcoin OR cryptocurrenc * OR “distributed ledger*”) AND (GDPR OR “General Data Protection Regulation”))	114	Scopus, Web of Science, and Google Scholar	1. What issues public blockchain systems can lead to in relation to data subject’s rights and data protection principles provided by the GDPR? 2. What solutions have been proposed in the research literature to address the tension between public blockchain systems and the GDPR?	Focus on GDPR compliance issues and proposed solutions for data protection in public blockchain systems.

4.0 METHODOLOGY

The objective of conducting the SLR in this study is to identify relevant research related to the subject area, particularly in blockchain-based inter-organizational information sharing with data confidentiality protection and to thoroughly examine and interpret the findings. To conduct the SLR, we followed the guidelines from Kitchenham and Charters [22]. In addition, we also adopted the snowball search process proposed by Wohlin [23] to enhance the comprehensiveness of our search. The use of both techniques has been done before [24], and it provides more flexibility in searching relevant papers rather than relying solely on keyword-based searches.

4.1 Planning

To fulfil the objectives of this study, three research questions have been formulated to examine the current advancements in the subject area, specifically:

RQ1: What is the distribution of blockchain types and data storage strategies adopted by researchers for information sharing?
Motivation: The motivation behind RQ1 is to identify the trends in blockchain types and data storage strategies chosen by researchers to facilitate information sharing using blockchain. These trends provide insights into the primary quality factors researchers aim to address, such as scalability, transparency, immutability, and security.

RQ2: What application domains were covered in the study?
Motivation: The objective of RQ2 is to identify the application domains that are the subject of researchers' studies. The findings from this question will highlight which application domains are most explored by researchers.

RQ3: What techniques are used alongside blockchain to ensure information confidentiality in inter-organizational information sharing?
Motivation: The architectural design proposed with blockchain may be general in nature and may inherently address data confidentiality requirements. Therefore, this RQ3 aims to explore the techniques proposed by researchers for ensuring information confidentiality on blockchain from unauthorized access, even among trusted organizations.

RQ4: What scenarios are suitable for the proposed techniques?
Motivation: The aim of RQ4 is to understand how the proposed techniques align with specific contexts or scenarios, including particular security challenges, data types, and organizational policies. This alignment is crucial for the development of an architectural framework that addresses the underlying requirements and real-world applications.

4.2 Search Strategy

At the outset of this phase, selecting appropriate keywords is essential to ensure that the papers located and collected are aligned with the research objectives and effectively address the specified research questions. Accordingly, we identified key terms aligned with the research objectives: "blockchain," "information sharing," "confidentiality," and "inter-organizational," to generate the keywords: “blockchain” AND “information sharing” AND “confidentiality” AND “inter-organizational. However, after conducting a preliminary testing search using the combination of these keywords, we found that the number of papers retrieved was too limited. Therefore, synonymous keywords were selected to expand and diversify the scope of the literature search. As a result, we finalized the keywords and structured the search string as follows:

("information sharing" OR "data sharing" OR "record sharing" OR "information exchange" OR "data exchange" OR "record exchange") AND ("blockchain" OR "distributed ledger" OR "decentralized") AND ("confidentiality" OR "privacy" OR "security") AND ("inter-organizational" OR "cross-organizational" OR "inter-agency" OR "cross-agency")

We have selected eight digital indexing libraries, Web of Science, Scopus, IEEE Xplore, ACM Digital Library, ScienceDirect, Wiley, Taylor & Francis, and Springer, as our primary automatic search platforms, chosen for their credibility and influence in the academic and research communities. However, we used only the keywords during preliminary testing to search papers in ScienceDirect, as the database does not support more than eight keywords in a single search string. The secondary platform, Google Scholar, was used during the snowball search process. This platform was specifically chosen to complement the primary sources by identifying additional relevant research articles through citation tracking and references from the final included papers.

4.3 Study Selection

We aimed to find high-quality journals and conference proceedings, while excluding secondary studies such as review papers, books, white papers, theses, and presentations. The process of selecting papers is illustrated in Fig. 2. The numbers displayed in the figure represent the number of papers retrieved at each stage of the selection process. The time frame for the papers searched spans from 2009 to 2024. This starting point was chosen because blockchain was only introduced in 2008, and 2009 was selected as it is relevant to the time frame in which researchers began publishing papers related to this subject area. We used tools such as Paperpile and Microsoft Excel to assist us during the study selection process. Based on the initial search, we found a total of 1,554 papers.

Table 2: Exclusion and inclusion criteria for selecting study papers.

Exclusion Criteria	Inclusion Criteria
1. Not utilized blockchain technology. 2. Not secondary studies. 3. Not available to download.	1. The article considers the need for data confidentiality or privacy protection. 2. Provide architectural design. 3. Peer-review papers. 4. Article journal or proceeding conference. 5. Written in English.

After removing 35 duplicates, we were left with 1,519 papers. We then applied a filtering process based on the title and abstract, requiring the papers to involve the use of blockchain technology as part of the solution. As a result, out of the 1,519 papers, 1,476 were excluded, leaving us with 43 papers to be screened in full text. In order to ensure the papers are relevant to the subject area, we established a set of inclusion and exclusion criteria, as detailed in Table 2. After conducting a full-text review and filtering, we selected 31 papers as the study material. Next, we performed a snowball search using Google Scholar and selected 20 additional papers. In total, 51 papers were included in the primary study.

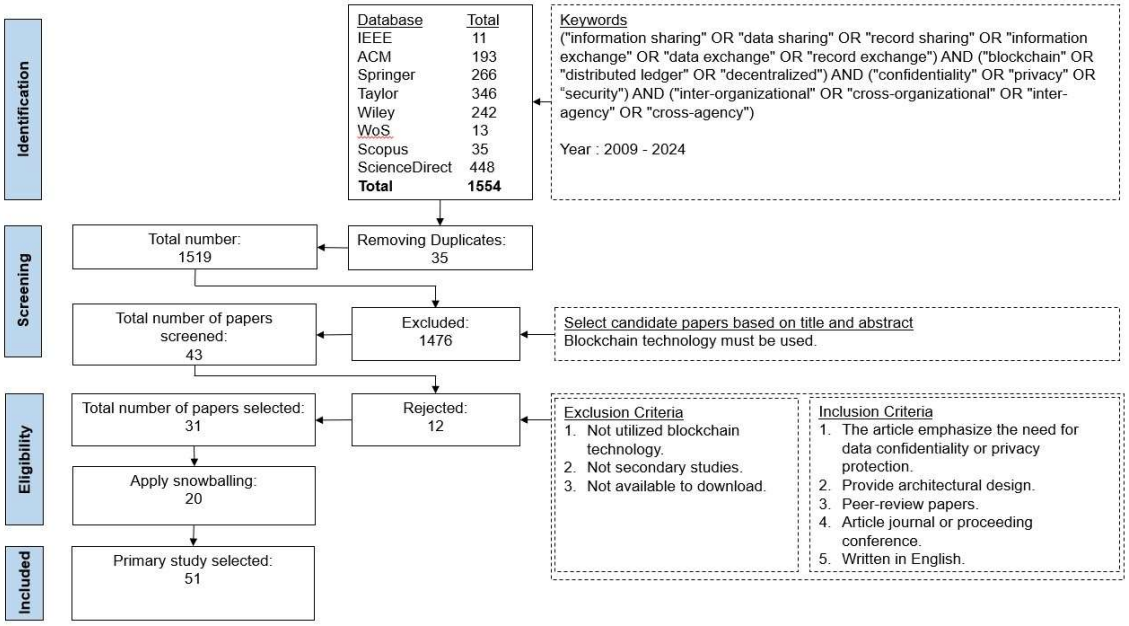

Fig. 2: The process of selecting study papers.

4.4 Data Extraction and Synthesis

In this phase, the first author conducted the data extraction process, systematically documented the findings in the designated data extraction fields, as outlined in Table 3. To ensure the accuracy and reliability of the extracted data, the second and third authors performed a rigorous cross-verification by randomly selecting papers and confirming that the recorded values accurately corresponded to the original sources.

4.5 Quality Assessment (QA)

QA was conducted to assess the quality standards of the articles selected for the study. The instrument used during the QA process was Kitchenham and Charters [22], a well-known and widely used instrument [25]. A quality checklist was developed, as outlined in Table 4, to assess whether the selected articles had sufficient merit to be included in this study. The results of the QA conducted are presented in Fig. 3.

Table 3: Data format extraction.

Data Item	Value
Paper ID	Code
Paper Title	Title of the paper
Domain	Specific application domain associated with the paper
Author Name	Author(s) of the paper
Publication Year	Full-year format
Publication Type	Conference paper or journal article
Country Name	Country of the first author
Region Name	Region name of the country
Architectural Design Approach	Blockchain design chosen for the information-sharing solution
Information Confidentiality Techniques	Techniques used alongside blockchain to ensure data confidentiality
Context of Techniques	Scenario associated with the technique

Table 4: Quality assessment checklist.

QA	Criteria	Description of checklist	Grading
QA1	Is the article related to information sharing between different organizations?	Yes, it is related to the subject. Partially, still within the context but not focus on organizational interest. No, not related at all.	Yes=1, Partial=0.5, No=0
QA2	Does the data confidentiality protection adopt an organizational-centric approach?	Yes, data access is controlled by a specific organizational policy. Partially, data access is controlled by a specific individual's discretion. No, data access is controlled by the built-in authorization mechanism in the blockchain or is not explicitly defined.	Yes=1, Partial=0.5, No=0
QA3	Does the article focus on any domain?	Yes, focus on a specific domain. Partially, it is generic and applicable to multiple domain. No, it does not applicable to any domain.	Yes=1, Partial=0.5, No=0
QA4	Do the authors explain the solution design?	Yes, it is explained clearly and supported by a working prototype. Partially, the design is discussed conceptually but lacks a working prototype. No, the solution design is not provided.	Yes=1, Partial=0.5, No=0
QA5	Is the solution supported by the results?	Yes, the solution is fully supported by the results, with clear evidence and validation. Partially, the solution is somewhat supported by the results, but relies primarily on assumptions. No, evaluation is not conducted.	Yes=1, Partial=0.5, No=0

The scoring scheme is based on the following criteria: A score of 'Yes' (1) is assigned if the article fully meets the outlined criteria. If the article partially meets the criteria or remains within the defined scope, it is assigned a score of 'Partial' (0.5). Lastly, a score of 'No' (0) is given if the article does not meet the required quality criteria.

Overall, an article that meets all criteria will receive a total score of 5, whereas an article that does not meet any criteria will receive a score of 0.

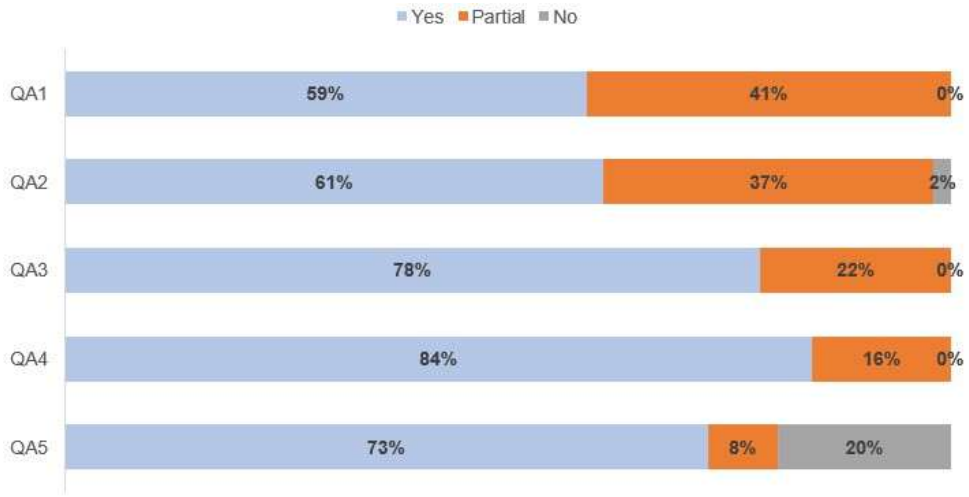

Fig. 3: Quality assessment results.

The QA1 criterion assesses whether the articles pertain to information sharing between organizations. The analysis identified 30 articles as directly relevant to this topic, while the remaining articles exhibit partial relevance. Similarly, based on the QA2 criterion, this study found that 31 articles adopt an organizational-centric approach, 19 articles focus on a user-centric approach, and only one article does not clearly specify its approach. Meanwhile, the QA3 criterion indicates that 40 articles focus on a specific application domain, whereas the remaining articles are more generic and adaptable to various domains. Next, QA4 assesses whether the authors propose a solution design, with the review revealing that 43 articles achieved a score of 1, while the remaining articles received a score of 0.5. Lastly, the fifth criterion, QA5, examines whether the proposed solution is supported by the results. The analysis found that 37 articles fully meet the requirement, four articles received a score of 0.5, and 10 articles did not include any evaluation. Overall, all 51 articles still align with the objectives of this study, and none were excluded from the analysis.

4.6 Primary Study Distributions

Overall, out of the 51 papers included, 14 are conference papers, while the remaining 37 are journal articles presented in Fig. 4.

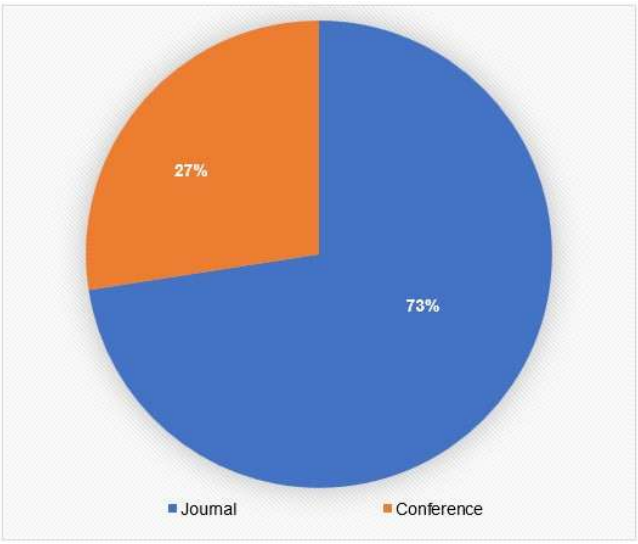

Fig. 4: Distribution of study papers by type.

4.7 Publication Year Overview

Fig. 5 depicts the range of publication years for the included papers, from 2018 to 2024. Research within this subject area has been steadily increasing, reflecting a growing interest among researchers in exploring information sharing methods through blockchain technology.

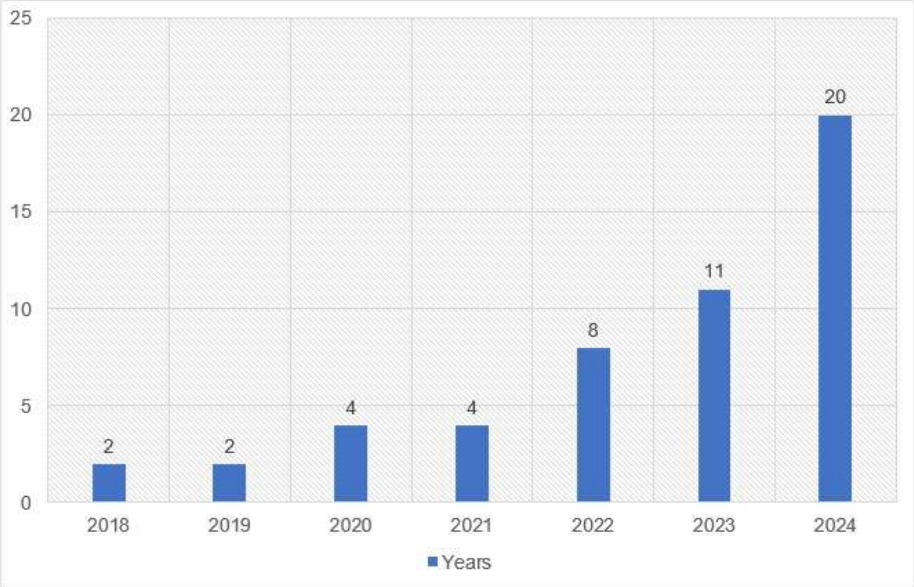

Fig. 5: Distribution of study papers by publication year.

4.8 Geographic Distribution

The distribution of papers based on the geographic location of the first author is shown in Fig. 6. The largest proportion of papers was published by East Asian authors, particularly from countries such as China and Taiwan. The second-highest contribution came from South Asia, with authors mostly from India, Pakistan, and Bangladesh. Additionally, regions such as the Middle East (including Saudi Arabia), North Africa (representing countries like Tunisia and Algeria), and Southeast Asia (with countries like Singapore) each accounted for 4% of the total papers. Other regions, including North America (United States), Southeastern Europe (Turkey), and Oceania (Australia), contributed 2% each to the overall publication count.

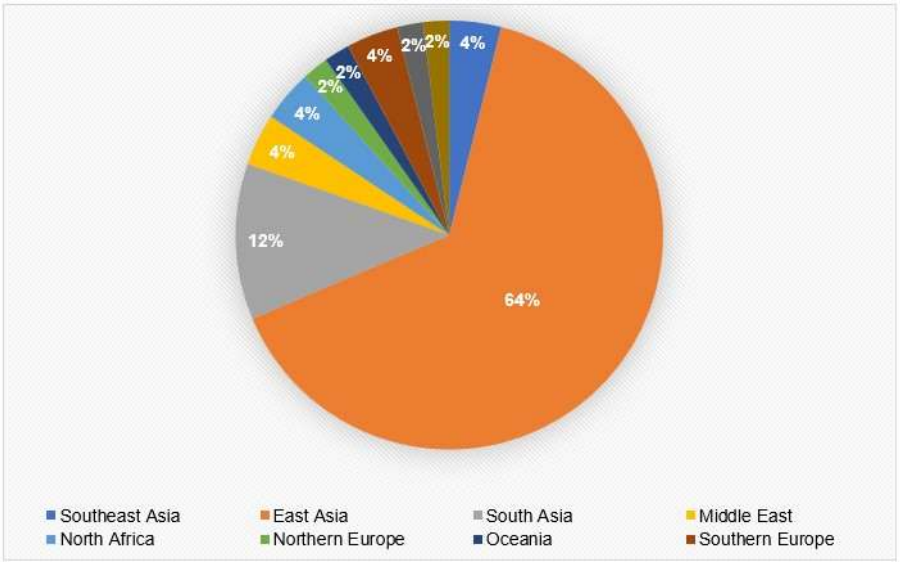

Fig. 6: Geographic distribution of study papers.

5.0 RESULT AND ANALYSIS

This section presents the findings from the full-text review, which address the research questions. For clarity, Table 5 provides the meanings of the numerous abbreviations used throughout this paper.

Table 5: Abbreviations

Abbreviation	Meaning
ABAC	Attribute-Based Access Control
ABE	Attribute-Based Encryption
AES	Advanced Encryption Standard
ALBS	Anti-Quantum Lattice-based Blind Signature
CO-RBAC	Collaborative Role-Based Access Control
DO-DB	Document-Oriented Database
FL	Federated Learning
GBAC	Group-Based Access Control
HE	Homomorphic Encryption
JSON	JavaScript Object Notation
LSSS	Linear Secret Sharing Scheme
P2P File Storage	Peer-to-Peer File Storage
PRE	Proxy Re-Encryption
RBAC	Role-Based Access Control
RS	Ring Signature
RSA	Rivest–Shamir–Adleman
SSE	Symmetric Search Encryption
XML	Extensible Markup Language
ZKP	Zero-Knowledge Proof

5.1 Distribution of blockchain types and data storage strategies

To provide a clearer overview, we have organized the study findings on blockchain types and storage strategies into Table 6.

5.1.1 Blockchain Types

49% of researchers choose permissioned blockchain as a platform because, by design, it does not allow anonymous users to join the network. Each participant must be identified, enhancing information security. It also ensures privacy, as only invited parties can participate in the blockchain network. Another 33% of researchers prefer permissionless blockchain since it effectively incentivizes contributors, particularly in systems designed with a user-centric approach. Meanwhile, 18% of researchers do not specify the type of blockchain in their papers. These papers are categorized as "Generic", as the proposed solutions are applicable to both types of blockchains.

5.1.2 Storage Strategies

Due to the scalability challenges associated with on-chain data storage in blockchain systems, researchers have adopted off-chain storage strategies as an alternative solution. On-chain storage involves storing original data directly within the blockchain ledger. In this context, original data refers to information that can be accessed and utilized directly, without requiring additional retrieval or processing from external sources. This excludes elements like hash addresses or decryption keys, which serve as references to or depend on external data storage. While some studies explicitly detail the specific off-chain storage methods used, others do not provide such specifications. Consequently, these studies are categorized more broadly under the general classification of "generic off-chain" data storage. Some researchers adopt a hybrid approach, storing smaller original data on-chain while keeping larger data off-chain. Studies employing this approach are categorized under the hybrid storage classification. Meanwhile, if the study paper does not specify where the original data is stored, we assume that the data is stored on-chain.

Various off-chain storage methods identified in recent studies can be categorized into P2P file storage, document-oriented databases, internal storage, and cloud servers. P2P file storage is based on the concept of decentralized file sharing, removing the need for a centralized server by distributing or replicating files across multiple peers. Notable P2P file storage technologies include InterPlanetary File Storage (IPFS), Filecoin, and Storj. Additionally, document-oriented databases such as CouchDB and MongoDB are favored for their ability to efficiently store files in formats like JSON and XML. For some researchers, internal storage remains the preferred

method for safeguarding highly sensitive information from unauthorized access. In contrast, researchers increasingly favour cloud servers for organizations due to their cost-effectiveness, as they mitigate the need for significant investment in on-premise infrastructure by offering flexible, subscription-based services from trusted and certified cloud providers.

The results, as illustrated in Fig. 7, show that off-chain storage has become the most popular choice among researchers using permissionless and generic blockchain types. However, we found minimal differences for permissioned blockchains, with only 7% variation in the use of on-chain versus off-chain storage. This is because permissioned blockchains offer higher scalability compared to permissionless blockchains and do not require a mining process to generate blocks, which typically takes more time to process. Overall, researchers tend to prefer off-chain storage over on-chain storage, with 57% opting for off-chain and 41% for on-chain across both types of blockchain. However, only a single study proposed the implementation of a hybrid storage approach, and this was limited to permissioned blockchains.

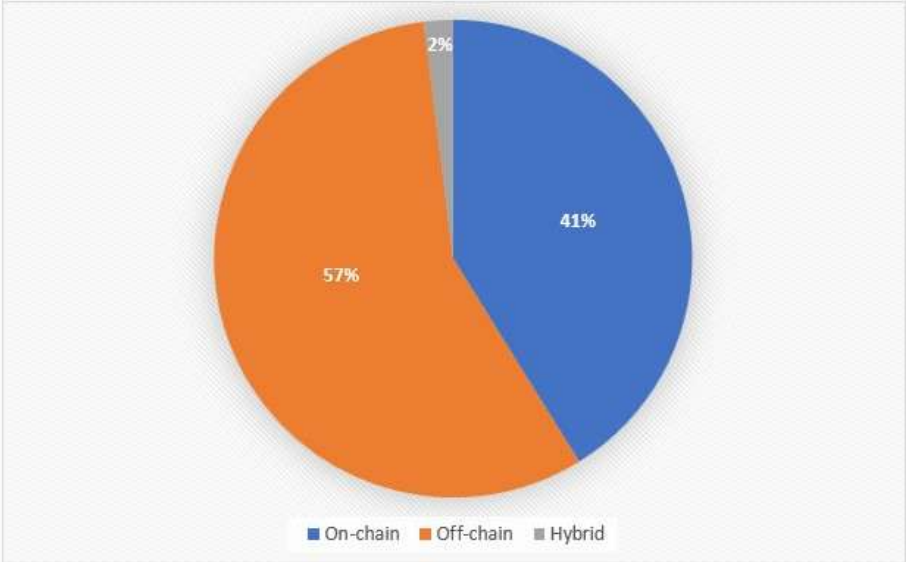

Fig. 7: Distribution of storage strategies: on-chain, off-chain, and hybrid.

Table 6: Distribution of blockchain types and data storage in study papers.

Blockchain Type	Data Storage	Study Papers	Total	Percentage
Permisionless	**On-chain**	[26]–[28]	3	6%
	Off-chain			27%
	P2P file storage	[9], [29]–[36]	9	
	DO-DB	[37]	1	
	Internal	[38]–[40]	3	
	Cloud Server	[41]	1	
	Total			33%
Permissioned	**On-chain**	[42]–[55]	14	27%
	Off-chain			20%
	Generic	[10], [56]–[59]	5	
	P2P file storage	[60]–[62]	3	
	Internal	[63], [64]	2	
	Hybrid	[65]	1	2%
	Total			49%
Generic	**On-chain**	[66]–[69]	4	8%
	Off-chain			10%
	P2P file storage	[70]	1	
	Internal	[71]	1	
	Cloud Server	[72]–[74]	3	
	Total			18%

5.2 Application Domain

This section presents the results for answering RQ2, which have been organized in Table 7. Some researchers did not explicitly state the application domain in their papers, but the subject of their studies tends to be more generic and applicable to other application domains, such as access control. Therefore, we have categorized their papers under the "Generic" application domain. The results show that information sharing in the healthcare domain is the most widely studied application domain, with 42%, followed by generic at 14%, then business and supply chain, each with 6%. This is followed by energy, transportation, Cloud, and IoT at 4%, and others at 2%.

Table 7: Paper grouped by application domain

Application Domain	Study Papers	Total	Percentage
Healthcare	[9], [10], [26], [28], [29], [32]–[35], [37], [38], [40]–[42], [47], [62], [66], [69]–[72], [74]	22	43%
Business	[53], [58], [60]	3	6%
Smart Society	[57]	1	2%
Trading	[30]	1	2%
Energy	[48], [64]	2	4%
Transportation	[52], [63]	2	4%
Government	[39]	1	2%
Supply Chain	[43], [49], [75]	3	6%
Emergency	[51]	1	2%
Electronic	[54]	1	2%
IoT	[46], [50]	2	4%
Vehicular	[31]	1	2%
Construction	[56]	1	2%
Financial	[67]	1	2%
Cloud	[61], [73]	2	4%
Generic	[27], [36], [44], [45], [55], [59], [68]	7	13%

5.3 Techniques for Confidential Inter-Organizational Data Sharing on Blockchain

Based on the analysis conducted on the study papers, several papers proposed a combination of multiple techniques, while others focused on only one specific technique. To better understand each approach, we categorized the techniques into several groups according to their characteristics, including privacy-preserving, access control, data perturbation, reversible ciphering, and isolated area, as illustrated in Fig. 8. Therefore, the same reference may be cited repeatedly under different categories, as it employs more than one technique in different categories.

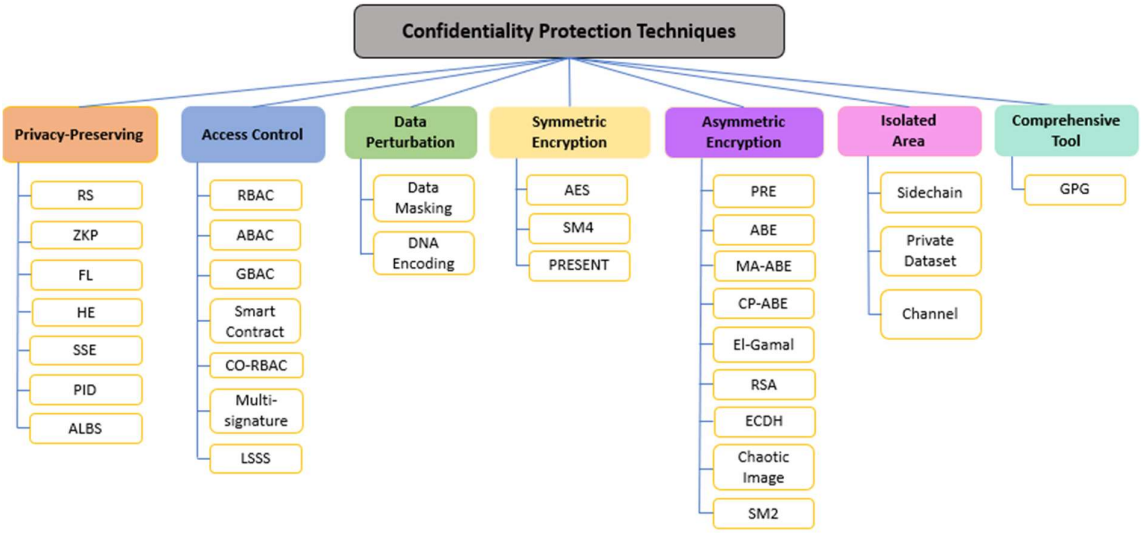

Fig. 8: Taxonomy of confidentiality protection techniques applied to blockchain technology.

5.3.1 Privacy-Preserving

Information protection is fundamentally linked to privacy, particularly concerning the disclosure of personal or sensitive information. Additionally, privacy involves safeguarding the user's identity, ensuring it remains confidential and anonymous, and preventing it from being exposed or recognized by unauthorized parties. The authors of [69] created a pseudo identity for each organization and user as a method to protect identity. The pseudo identity is created by XOR-ing the user's true identity with a randomly chosen value, appending that random value, and then encrypting the result. This encrypted pseudo identity is used during interactions and may be referenced on the blockchain, allowing the system to protect user privacy while retaining the ability to trace the real identity through a trusted authority.

In the digital world, a digital signature is crucial for ensuring that the message received is authentic and originates from the sender. However, traditional digital signatures typically expose the sender's identity. The authors of [61], [72] suggested using RS to maintain the sender's anonymity while simultaneously assuring the recipient of the message's legitimacy. Technically, an RS involves each member of the group contributing their public keys, partial signatures, and random values. The verifier can validate the signature without knowing the actual identity of the signer, ensuring anonymity. Meanwhile, the authors in [26] proposed an anti-quantum lattice-based blind signature (ALBS) to secure sensitive information while protecting privacy from both classical and quantum attackers. A blind signature allows the user to get information signed by the signer without the signer seeing the contents of the information. This method is specifically designed to be quantum-resistant. Nevertheless, anonymity constitutes a substantial challenge in scenarios that require verification of the sender's identity, particularly in authentication mechanisms.

The authors in [53] propose the ZKP technique to prove that a blockchain transaction is valid without revealing any sensitive information. Techniques like ZKP allow an entity to prove that a fact is true to a verifier without disclosing additional information such as sender, receiver, or transaction amount. The scheme utilized in this paper is Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (ZK-SNARK). Through this scheme, the prover constructs a mathematical proof derived from the secret information they possess. The verifier can then confirm the validity of the proof without needing to know the actual information. This process occurs without repeated communication, and the proof is both concise and quickly verifiable.

Meanwhile, FL and HE have become key areas of research focused on safeguarding sensitive information. Instead of producing output in the form of raw data, both techniques output only aggregated data to the public, preserving privacy and minimizing the risk of exposure. The authors of [48], [52], [53], [59], [64], [67] utilized HE to protect the original data by storing it in ciphertext form while enabling computational operations to be performed directly on the encrypted data. HE is a technique that enables computational operations to be performed on encrypted data (ciphertext) without revealing the underlying plaintext. This method generates only aggregated results, preserving the privacy of the original data.

Meanwhile, the authors of [46], [50], [55], [68] used the FL technique, which focuses on machine learning and allows models to be trained locally on individual devices or servers, eliminating the need for sensitive data to leave its original location. This method preserves data privacy while still facilitating the development of machine learning models. After local training, the updated models are sent to a central server, where they are aggregated to create a global model. The blockchain's role is to secure multi-party computation, facilitate model sharing, and incentivize cross-organization collaboration through cryptocurrency rewards.

Typically, searching the content on encrypted data is challenging because it is unreadable and inaccessible. Without decryption, traditional search techniques cannot be directly applied to ciphertext. This limitation makes it difficult to retrieve specific information or perform operations on encrypted data. To address this, the authors of [60], [74] used the SSE technique, which enables secure searches within encrypted datasets, allowing users to search for specific keywords without exposing the underlying data. With SSE, the data owner creates an encrypted index that maps specific attributes to the encrypted data. When a user submits a query with keywords, the system searches the corresponding encrypted index to locate the relevant record. The search results point to the encrypted data without revealing its contents.

5.3.2 Access Control

Access control is a mechanism that implements authorization decisions within a system. It defines and manages the permissions granted to authenticated entities, determining what actions are allowed on the resources. The study identifies Role-Based Access Control (RBAC) as a technique where permissions to perform specific operations are assigned to roles rather than individuals [33], [43], [45], [47], [49], [50], [60]. Entities associated with a particular role can perform only the operations permitted for that role. Similarly, the authors of [40] introduced the term Group-Based Access Control (GBAC), where permissions are granted to groups, a concept closely resembling RBAC. In contrast to RBAC, Attribute-Based Access Control (ABAC) has gained significant attention, as permissions are granted based on the attributes or characteristics of the subject, object, operation, and environment [27], [49], [54], [58], [59]. While ABAC is more complex than RBAC, it offers greater flexibility in policy decision-making. The authors of [61] combine Linear Secret Sharing Scheme (LSSS) with Attribute-Based

Encryption (ABE), which acts as the access structure. In LSSS, the access structure is typically represented in matrix form. The LSSS matrix helps enforce the access policy by mapping the thresholds to specific attributes. Each threshold must be satisfied for access to be granted, and the matrix ensures that only users with the required combination of attributes can decrypt or access the data. In a decentralized environment, the multi-signature technique is a viable option for enhancing security. The authors of [45] utilized a technique where multiple signatures from different parties are required to approve an action, rather than relying on a single signature from one party. These signatures are used in conjunction with RBAC to implement Collaborative Role-Based Access Control (CO-RBAC), ensuring that permissions are granted only if the requester obtains valid signatures from all involved organizations.

5.3.3 Data Perturbation

Data can be stored in an altered format rather than its original form, enabling statistical analysis while employing a method called data perturbation. This method differs from traditional encryption, instead of rendering the data completely unreadable and indecipherable, data perturbation obscures the actual values while preserving the structure and format of the data. This allows an understanding of the data's context without exposing its precise content. Techniques found in study papers under data perturbation include data masking, with Deoxyribonucleic Acid (DNA) encoding also explored as a novel approach in certain contexts. The authors of [58], [70] apply the data masking technique, which obscures the actual data while preserving its structure and format, ensuring that the original values remain hidden. Data masking is implemented through techniques such as replacing sensitive data with fictitious or scrambled values, generalizing specific data, modifying numerical values, hiding parts of the data, or adding/removing data elements to obscure the original information. Meanwhile, the authors of [66] used DNA encoding, inspired by the genetic code, to provide an extra layer of obfuscation to the encrypted data. This method means that even after the data is decrypted, it still requires the reassembly of fragments before it can revert to its original information.

5.3.4 Symmetric Encryption

As a measure for complete data protection, encryption is one of the most effective techniques and often serves as the last line of defence for ensuring data confidentiality. This technique involves completely altering the structure and format of the original data, rendering it unreadable and incomprehensible to unauthorized individuals. Therefore, even if the data is stolen or successfully intercepted, the adversary still cannot read it without the decryption key. The Advanced Encryption Standard (AES), a type of encryption under symmetric encryption, is a popular choice among the authors of [29], [31], [32], [42], [48], [73]. AES is known as a block cipher and supports a key size of up to 256 bits, providing stronger security. However, AES 128 bits shows better performance in terms of execution time compared to the 256-bit version. A study by the authors of [31] also presented a comparison with other types of encryption, such as Triple Data Encryption Standard (3DES) and the Affine Cipher, which do not demonstrate performance comparable to AES.

Meanwhile, the authors of [33] utilize SM4, which relies on Elliptic Curve Cryptography (ECC). It only supports a 128-bit key size. SM4 is less widely adopted than AES, but it is considered cryptographically secure and offers a comparable level of protection within its intended use context. However, it has undergone less global scrutiny compared to AES. Another encryption technique used by researchers is PRESENT [63], which is ultra-lightweight and ideal for hardware-constrained devices such as Radio-frequency Identification (RFID). The key size generated is either 80 or 128 bits, and the block size is 64 bits. Since PRESENT uses a smaller block size and key size, it does not require as high processing power as AES. All of the researchers used the mentioned encryption techniques to encrypt large-sized actual data. However, all these symmetric encryption techniques face challenges in securely sharing the secret key with multiple recipients and lack the capability to authenticate the data owner's identity.

5.3.5 Asymmetric Encryption

Several researchers have explored various techniques under asymmetric encryption, whose primary role is as a key delegation mechanism for managing symmetric key, enabling digital signatures, or encrypting data [56], [57]. As comparison, asymmetric encryption performance is not as efficient as symmetric encryption when it comes to encrypting large volumes of data or operating on low-power devices. Therefore, it is only suitable for encrypting small data such as secret keys. The mechanism used by the authors were encrypt the secret key with data owner's public key and only can be encrypted by using data owner's private key. To share the secret key, the data owner needs to first decrypt the secret key, then re-encrypt it using the receiver's public key before transmitting it. The receiver can then decrypt the secret key using their private key. One such technique is Rivest–Shamir–Adleman (RSA), a traditional cryptographic method that remains popular among the authors of [29], [32], [47], [48]. It is based on the large integer factorization problem and uses a minimum key size of 2048 bits up to 4096 bits to provide strong security. To date, RSA remains recognized as secure, with no successful attempts to compromise

its cryptographic strength since its introduction in 1978. Meanwhile, the authors of [42] proposes the Elliptic Curve Diffie–Hellman (ECDH) encryption algorithm as a key exchange technique, which is based on the discrete logarithm problem and operates within the algebraic structure of elliptic curve point groups. It uses a smaller key size compared to RSA while maintaining an equivalent level of security. Consequently, ECDH offers improved performance compared to RSA, particularly in terms of computation speed and efficiency. Next, the authors of [66] proposes the ElGamal encryption algorithm, which is built upon the discrete logarithm problem over integer, to encrypt two data fragments after the original data has been divided in half. This approach differs slightly in that the ElGamal algorithm is applied directly to encrypt the data itself, rather than employing a symmetric key for data encryption. The key size used in this study is 1024 bits, while the size of the data fragments depends on the size of the original data, such as an X-ray image. Compared to RSA, ElGamal typically produces a larger ciphertext than the original plaintext because it outputs two values per encryption and includes additional randomness. the authors of [33] employed the SM2 encryption algorithm, which shares similarities with ECDH, but mainly used for digital signature than key exchange. In this study, the SM2 algorithm is employed as a digital signature scheme to verify the authenticity of the data.

Meanwhile, the authors of [35], [69] discusses the use of PRE as a key delegation method from the data owner to the recipient. This technique requires an entity to act as an intermediary or proxy to perform re-encryption on the ciphertext without needing to know its contents. It can also be considered a form of double encryption. In this way, the owner does not need to perform the decryption and re-encryption process on the data intended for sharing with the recipient, as in RSA, instead the task of re-encrypting the ciphertext is delegated to a third party with higher processing power, such as a cloud server. In contrast, the authors of [30], [44], [61], [72] uses ABE, a cryptographic technique that enables fine-grained access control. In ABE, data is encrypted in such a way that only individuals with attributes satisfying the defined access policy can decrypt it. This approach ensures that decryption is restricted to users who possess the necessary characteristics or credentials. There are various variants of ABE, the authors of [30] uses the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) variant in which a single authority manages all attributes, while the authors of [44] uses the Multi-Authority Attribute-Based Encryption (MA-ABE) variant where attributes are issued by multiple independent authorities. A key characteristic of ABE is that encrypted data must be re-encrypted whenever there are changes to the attribute conditions. This poses a challenge in a blockchain environment, where existing data cannot be altered. Instead, a new version of the data must be recorded in a subsequent block. As a result, the previous data may no longer be decryptable due to outdated attributes condition, which could compromise traceability. Another technique for transforming plaintext into obfuscated data is through the use of chaotic images as proposed by the authors of [71], inspired by nonlinear dynamics and chaos theory. In this approach, sensitive event log data is categorized by attribute importance, converted into encrypted color images using chaotic parameters via the Log-image Data Conversion (L-IDC) algorithm, and then merged and processed using the Image Merge Diffusion Encryption (IMDE) algorithm, which applies diffusion and confusion techniques to increase the security of the encrypted image. A unique image ID is generated, stored on-chain via smart contracts, while the encrypted images are stored off-chain within each organization, ensuring lightweight blockchain use and data privacy.

5.3.6 Isolated Area

Each blockchain type features a unique data storage mechanism and distinct approaches to node interaction within the network. The authors of [28], [47], [53] proposes utilizing a sidechain blockchain to store sensitive data, while public data is maintained on the mainchain. This approach enhances blockchain scalability, improving access efficiency for medical officers. Strict access control measures are enforced to safeguard medical data privacy against internal threats. Quite a similar concept, the authors of [52] employs a technique of separating channels when data does not need to be shared with all nodes. Nodes are grouped into specific channels, and only nodes within a given channel can access the data, ensuring controlled visibility and enhanced privacy. Additionally, the authors of [29] adopts a private dataset technique to protect data privacy from unauthorized nodes. With this method, only authorized nodes can access the original data, while the hash values are replicated to all nodes including unauthorized nodes, to ensure immutability and integrity checking.

5.3.7 Comprehensive Tool

A comprehensive tool is a software solution built on well-established and trusted cryptographic algorithms, widely recognized and adopted for secure applications in real-world environments. The tool identified in this study for encrypting image files is Gnu Privacy Guard (GPG), as proposed by the authors of [9]. GPG is an open-source implementation of the OpenPGP standard. It does not invent a new algorithm but instead uses established cryptographic algorithms such as AES and RSA to achieve its functionality. The proposed solution allows the sharing of image files from a doctor to a patient by encrypting the file using the patient's public key, and the encrypted file is stored in IPFS. It can only be decrypted using the patient's private key. Blockchain is utilized for access control and for tracing image files based on their IPFS hash addresses, ensuring both security and traceability throughout the file's lifecycle.

5.4 Scenarios Suited to the Proposed Techniques

The techniques outlined aim to address specific needs or contexts, emphasizing the importance of aligning their usage with particular scenarios. Based on the analysis of the study papers, we synthesized the findings and categorized the techniques according to relevant scenarios to enhance clarity and ensure their suitability for the intended purpose, as summarized in Table 8. It is noteworthy that the majority of the studies do not explicitly specify the scenarios appropriate for the techniques they employ. We identified these scenarios by conducting a detailed analysis of their proposed solutions and correlating the intended requirements with relevant use case scenarios. This section indirectly addresses RQ4 by providing detailed insights into the scenarios and their corresponding techniques. Some techniques overlap across multiple scenarios due to their versatile characteristics, making them applicable in various contexts.

Table 8: List of scenarios related to data protection techniques for confidentiality.

ID	Scenario	Techniques	Use Case
S1	Identity and privacy are protected through anonymity.	RS, ZKP, PID	Voting, Healthcare
S2	Operational authorization is managed by fine-grained access control.	ABAC, LSSS, Smart Contract	Heterogeneous systems
S3	Operational authorization is managed by coarse-grained access control.	RBAC, GBAC, CO-RBAC, Multi-signature, Smart Contract	Homogeneous systems
S4	The output is generated in the form of aggregated data.	HE, FL	Data mining, Machine Learning
S5	As a method to exchange encryption keys or delegate decryption rights to authorized parties.	RSA, SM2, ECDH, ElGamal, PRE, ABE, CP-ABE, MA-ABE, GPG	Email forwarding, File sharing
S6	Efficiently transformed a small-sized dataset into an unreadable form in a constrained environment.	PRESENT	IoT, Low-power devices
S7	Efficiently transformed a small-sized dataset into an unreadable form in a resource-rich environment.	RSA, SM2, ElGamal, ABE, CP-ABE, MA-ABE, HE, GPG	Military, Banking, Cloud services
S8	Efficiently transformed a large-sized dataset in bulk into an unreadable form.	AES, SM4, Chaotic image, GPG	General purpose, Video Surveillance
S9	Information is hidden through complexity.	Data masking, DNA encoding	Personally identifiable information
S10	Enable encrypted data to be searched while preserving confidentiality.	SSE	Cloud storage
S11	Sensitive information is isolated through architectural separation mechanisms.	Sidechain, private dataset, channel	Blockchain

Scenario S1 is particularly applicable for organizations that prioritize data authenticity and legitimacy while maintaining the anonymity of user identities. This is especially relevant in domains such as healthcare, where patient confidentiality is critical yet secure communication of diagnostic information, such as laboratory test results, is essential. Methods under this scenario enable verification of data authenticity without requiring explicit identification of user identities, thereby ensuring both privacy and validity.

A review of existing studies highlights that scenarios requiring detailed, specific permissions align with the fine-grained access control approach, as described in Scenario S2. This approach grants access permissions based

on attributes such as the subject, action, object, and environment, allowing access only to users who meet predefined criteria in the access control policy. While this method provides precise and robust authorization, it becomes increasingly complex and challenging to manage as policies grow more intricate. With the presence of smart contracts, the authorization process can be performed automatically in a decentralized manner. The combination of smart contracts with ABAC can further enhance the security and efficiency of the system. Scenario S2 is particularly appropriate for use in systems that require a high level of security and are heterogeneous in nature.

Conversely, for situations where the authorization process does not demand highly detailed permissions, the coarse-grained access control approach, outlined in Scenario S3, is more suitable. This method assigns permissions to groups or roles, and users inherit access based on their assigned roles. Although this approach is simpler and more manageable, it can lead to over-privileged access, as users receive all permissions associated with their roles. This may conflict with the principle of least privilege, posing potential security risks. Meanwhile, multi-signature ensures that authorization decisions are made based on mutual agreement among authorized parties, to prevent decision-making errors or deliberate malicious actions. Scenario S3 is particularly appropriate for homogeneous environments where applications have relatively uniform access requirements across different roles.

Aggregated data offers a practical solution in scenarios where safeguarding original data is crucial due to privacy concerns. By concealing raw data, aggregated information remains valuable for statistical analysis and machine learning model development. Techniques outlined in Scenario S4 are designed to address this need, enabling the sharing of insights without exposing the underlying data. This approach strikes a balance between preserving data privacy and allowing organizations to contribute meaningful and actionable information for statistical and analytical applications.

Scenario S5 aims for the case that key delegation is required. Key delegation refers to the process of securely granting access to a secret key, commonly a symmetric key to authorized recipients. This process is also known as Key Encapsulation Mechanism (KEM). A commonly adopted mainstream technique is where the secret key is encapsulated directly using the delegatee's public key by the data owner, and it can then be decrypted using the delegatee's private key, such as RSA, ElGamal and SM2. Meanwhile, techniques such as PRE are suitable for implementation in resource-constrained environments like mobile phones, as they offload the encryption process to a third party, whereas ABE can be used in environments that prioritize a higher level of security. Among the application domains that involve secret key exchange are email forwarding, file sharing, and secure messaging.

We identified that the techniques described in Scenario S6 are suitable for encrypting small-sized data in resource-constrained environments. Techniques such as PRESENT are efficient for use on low-power devices like RFID systems, IoT nodes, and smart cards. However, PRESENT is not ideal for long-term or high-security applications, as its relatively small key size may introduce vulnerabilities, particularly to brute-force attacks and differential cryptanalysis especially as hardware capabilities continue to advance.

In contrast, the techniques identified in Scenario S7 are also suitable for encrypting small-sized data but are designed for resource-rich environments. They typically require more powerful CPUs, sufficient RAM, or cryptographic co-processors to operate efficiently. These techniques offer stronger cryptographic guarantees and are better suited for high-security applications, providing more robust protection than those used in Scenario S6.

Although blockchain is inherently designed to promote data transparency among participants, certain scenarios demand confidentiality, thereby requiring organizations to avoid storing data in plaintext. In such cases, the data may be large in size, such as images, videos, or documents, which necessitates the use of efficient techniques, as outlined in Scenario S8. Among the techniques considered in this scenario, AES is regarded as the most credible due to its long-standing global adoption since its standardization in 2001. Nevertheless, SM4 has also been formally recognized as a national encryption standard by the People's Republic of China since 2016. Both techniques are designed for general-purpose use and can be applied in different domains, as long as the devices have high computational capability.

In scenarios where it is crucial to conceal the actual information while maintaining its recognizable structure and format, the techniques outlined in Scenario S9 provide a practical solution. Unlike encryption, which alters the data structure entirely, these techniques preserve the original format, allowing for interpretability. While not fully concealing the data pattern, the techniques obfuscate sensitive elements to ensure privacy. This approach guarantees data privacy while also validating the data's integrity and contextual relevance to the recipient.

Searching encrypted data is inherently challenging because the data is stored in ciphertext form. To address this, scenarios like S10 are referred, enabling encrypted data to remain searchable while still preserving the confidentiality of the information. Techniques such as SSE facilitate this functionality by allowing a search token, also known as a trapdoor, to be generated by the user along with the desired keyword. The server uses this token to search the encrypted index and returns the matching ciphertext to the user without learning the content of the token or the plaintext data. The user can then decrypt the data using the same symmetric key, ensuring both security and searchability.

Scenario S11 allows sensitive information to be isolated from general access, ensuring that only authorized parties can access it. Research studies have demonstrated that blockchain technology provides essential features to enable this capability, including sidechains, private datasets, and channels. However, the availability of these features is contingent upon the specific blockchain platform in use, as not all platforms support them. For instance,

sidechains are supported by Ethereum, Polkadot, and Cosmos, while private datasets and channels are features of permissioned blockchain platforms such as Hyperledger Fabric, R3 Corda, and Quorum.

6.0 FINDING AND GAPS IDENTIFIED FROM STUDY PAPERS

In this section, we summarize the findings from the study papers and present some gaps in confidentiality protection techniques in blockchain. In particular, our primary focus is to uncover current strategies for protecting information on the blockchain from the perspective of inter-organizational information sharing. We identified that the techniques used by researchers to protect the confidentiality of information can be adapted to eleven scenarios, depending on the suitability of the application. However, we identified the following gap in the existing research:

- **Lack of organizational-centric approach**: Most of the authors emphasize that adopting a user-centric approach to inter-organizational information sharing is essential in application domains such as healthcare, mainly due to legal frameworks like the GDPR, which grants data owners control over their data accessibility. However, this approach is not very suitable in an organizational-centric context, where data accessibility cannot be determined at an individual's discretion, but rather based on organizational policies. Consider the case that the level of trust among organizations varies. An organization that is fully trusted may be allowed to view all information, while an organization that is not fully trusted may face restrictions in accessing certain information. Such policies must be determined by the organization itself and cannot be bypassed by the administrator without approval from the organization's top management. Therefore, an organizational-centric approach is necessary for such a scenario.
- **Lack of decision-making model**: It is essential to recognize that the selection of techniques must be aligned with the specific use case or domain requirements. Not all techniques are universally applicable. For example, methods prioritizing anonymity may not be suitable for organizations emphasizing non-repudiation, as non-repudiation requires that all parties involved be identifiable to ensure accountability and traceability. However, combining multiple techniques to address various scenarios should be considered, as relying solely on blockchain does not guarantee data confidentiality. For example, combining RBAC and ABAC can result in a robust access control mechanism. To the best of our knowledge, there is currently no established decision-making model that systematically guides developers in selecting an appropriate technique, or a combination of techniques, tailored to a specific domain or use case.
- **Lack of time-bound access control**: The majority of authors do not address techniques that are suitable for scenarios requiring time-bound access enforcement. The justification for the requirement of time-bound access control is to reduce the risk of information being misused for purposes beyond what is authorized, and to support subscription and licensing models that specify access to information is allowed only within a valid license period. The mechanism for time-bound permission must be enforced automatically, without requiring the data owner to manually revoke permissions. Although ABAC and ABE are capable of enforcing time constraints through attributes, such mechanisms are generally high-level or generic in nature and tend to be inefficient when applied to individual pieces of information. Applying unique time constraints per data item can become complex and inefficient, particularly if the access policy needs to be dynamically updated or evaluated at a fine-grained level. Moreover, Time attributes in ABE are usually static, making the dynamic enforcement of expiration or revocation a non-trivial task.
- **Lack of content-based access control**: Information stored on the blockchain is well-known permanent and cannot be deleted. Assume that the information is indeed confidential and protected through encryption, it can still be shared using techniques such as those in S5 and S8. However, certain parts of the same dataset may be considered top secret and must not be shared at all. For example, in a dataset containing the attributes *name*, *identification number*, and *address*, only the *address* is labeled as top secret, while the *name* and *identification number* can be disclosed. The list of attributes labeled as top secret may change over time. Based on an analysis of existing studies, no dynamic content-based access control method has been identified, highlighting an opportunity for further research.

7.0 RECOMMENDATION

Based on the analysis of confidentiality protection techniques in blockchain, as identified in the reviewed studies, and their suitability for specific scenario requirements, we propose that the implementation of sensitive information sharing between organizations using blockchain technology can be guided by the decision-making model illustrated in Fig. 9. The model consists of a series of questions divided into three phases: Phase A (green), Phase B (yellow), and Phase C (blue).

Phase A. Determine the suitability of blockchain for information sharing: The first four questions aim to evaluate whether blockchain is suitable for inter organizational information sharing. Meanwhile, the final question in this phase is intended to determine which blockchain platform is most suitable for use.

Q1: Is a platform required for sharing data between organizations? - If yes, proceed to the next question. Otherwise, do not use blockchain.
Q2: Do all participating organizations willing to contribute their data to the shared platform? - If yes, proceed to the next question. Otherwise, do not use blockchain.
Q3: Do all participating organizations trust the platform as the resilient source of truth? - If yes, proceed to the next question. Otherwise, do not use blockchain.
Q4: Do all organizations consent to the involvement of a trusted third party? - If no, proceed to the next part. Otherwise, do not use blockchain.
Q5: Are trusted organizations allowed to join the platform? - If yes, use a public blockchain. Otherwise, use a consortium blockchain. A private blockchain is not considered in this context, as it is unsuitable for inter-organizational information sharing due to being managed by a single organization.

Phase B. Choose the appropriate techniques for confidentiality protection: Determine the level and type of protection to be achieved for sensitive information using the provided set of questions. Each question that is relevant to the requirement will point to an appropriate scenario, and the corresponding protection techniques can be referred to within that scenario, as shown in Table 8.

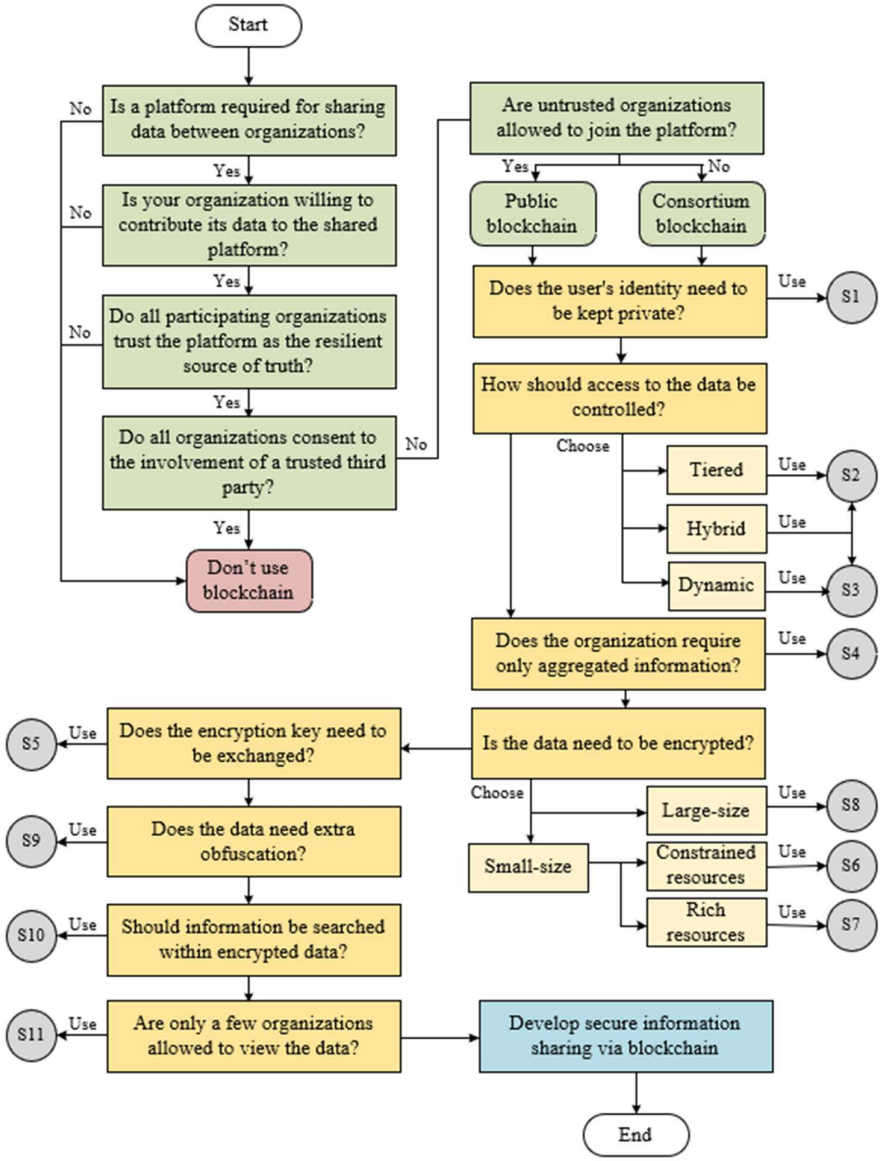

Fig. 9: A decision-making model for sharing sensitive information using blockchain

Q1: Does the user's identity need to be kept private? - If this question is relevant to the organizations, use the techniques listed in scenario S1.
Q2: How should access to the data be controlled? - If this question is relevant to the organizations, determine which access control model should be used: tiered (coarse-grained access control), with techniques listed in Scenario S2; dynamic (fine-grained access control), with techniques listed in Scenario S3; or hybrid (a combination of both).
Q3: Does the organization require only aggregated information? - If this question is relevant to the organizations, use the techniques listed in scenario S4.
Q4: Is the data need to be encrypted? - If this question is relevant to the organizations, determine which encryption techniques should be used based on data size and available computer resources: If the data size is large, use techniques from Scenario S8. If the data is small but resources are constrained, choose techniques from Scenario S6. Otherwise, use techniques from Scenario S7.
Q5: Does the encryption key need to be exchanged? - If this question is relevant to the organizations, use the techniques listed in scenario S5.
Q6: Does the data need extra obfuscation? - If this question is relevant to the organizations, use the techniques listed in scenario S9.
Q7: Should information be searched within encrypted data? - If this question is relevant to the organizations, use the techniques listed in scenario S10.
Q8: Are only a few organizations allowed to view the data? - If this question is relevant to the organizations, use the techniques listed in scenario S11.

Phase C: Develop a blockchain-based solution for secure information sharing: After evaluation and planning have been carried out, a blockchain-based application should be developed together with the selected techniques.

8.0 LIMITATION OF THIS STUDY

The techniques discussed in this paper are limited to those identified through a SLR conducted using specific keywords relevant to the subject of study. We also applied the snowballing technique to the primary papers. As such, the listed techniques may not represent the state-of-the-art in confidentiality protection in the context of blockchain. Some relevant papers may have been excluded either because they did not appear in the keyword-based search or were inaccessible due to subscription restrictions. Additionally, some conclusions are made based on assumptions because they are not clearly stated in the paper, such as the type of blockchain used and the type of data storage employed. As a result, we classified them as generic types. Despite these limitations, this paper provides a useful overview of the techniques that have been explored by researchers and serves as a foundation for further investigation into additional methods.

9.0 CONCLUSION

This paper aims to investigate key studies on confidentiality protection techniques within blockchain-based inter-organizational information sharing. A total of 51 primary studies were selected from eight digital libraries and search engines. Findings reveal that most authors employ permissioned blockchains and off-chain storage for information-sharing solutions. Seven information protection techniques were identified and categorized: privacy-preserving methods, access control, data perturbation, symmetric encryption, asymmetric encryption, isolated areas, and comprehensive tools. These techniques are mapped to eleven scenarios, as detailed in Table 8. This study provides guidance on applying these techniques to specific contexts. Combining multiple methods can yield a more robust and comprehensive data protection strategy. The proposed techniques are adaptable for blockchain integration based on scenario requirements. To aid decision-making, a model is presented in Fig. 9. Future research should examine the synergy among these techniques to develop optimal solutions for secure information sharing.

REFERENCES

[1] C. Loebbecke, P. C. van Fenema, and P. Powell, "Managing inter-organizational knowledge sharing," *The Journal of Strategic Information Systems*, vol. 25, no. 1, pp. 4–14, Mar. 2016.
[2] J. Ramon Gil-Garcia, I. Chengalur-Smith, and P. Duchessi, "Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector," *European Journal of Information Systems*, vol. 16, no. 2, pp. 121–133, Apr. 2007.
[3] B. Lundgren and N. Moller, "Defining Information Security," *Science and Engineering Ethics*, vol. 25, no. 2, pp. 419–441, Apr. 2019.
[4] D. Puspasari, A. N. Hadiyanto, and S. Setiawan, "Inter-organizational data sharing: What issues should be considered?," in *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS*, Jakarta, Indonesia, 2021, pp. 181–186.

[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized Business Review*, p. 21260, 2008.
[6] W. Y. Leong, Y. Z. Leong, and W. S. Leong, “Enhancing Blockchain Security,” in *2024 IEEE Symposium on Wireless Technology & Applications (ISWTA)*, 2024, pp. 108–112.
[7] L. B. Elvas, C. Serrão, and J. C. Ferreira, “Sharing Health Information Using a Blockchain,” *Healthcare (Basel)*, vol. 11, no. 2, Jan. 2023.
[8] H. Gao, Z. Ma, S. Luo, Y. Xu, and Z. Wu, “BSSPD: A Blockchain-Based Security Sharing Scheme for Personal Data with Fine-Grained Access Control,” *Proc. Int. Wirel. Commun. Mob. Comput. Conf.*, vol. 2021, Feb. 2021.
[9] D. Kumari, A. S. Parmar, H. S. Goyal, K. Mishra, and S. Panda, “HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy preserving scalable health data,” *Comput. Netw.*, vol. 241, no. 110223, p. 110223, Mar. 2024.
[10] Z. Xiao *et al.*, “EMRShare: A Cross-organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain,” in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS 2018)*, 2018, pp. 998–1003.
[11] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, “Analysis of Blockchain technology: pros, cons and SWOT,” *Cluster Comput.*, vol. 22, no. 6, pp. 14743–14757, Nov. 2019.
[12] S. Kim, Y. Kwon, and S. Cho, “A survey of scalability solutions on blockchain,” *2018 International Conference on*, 2018.
[13] E. A. Franciscon, M. P. Nascimento, J. Granatyr, M. R. Weffort, O. R. Lessing, and E. E. Scalabrin, *A Systematic Literature Review of Blockchain Architectures Applied to Public Services*. IEEE, 2019.
[14] I. Weber *et al.*, “On availability for blockchain-based systems,” in *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, Hong Kong, Hong Kong, 2017, pp. 64–73.
[15] E. Politou, E. Alepis, C. Patsakis, F. Casino, and M. Alazab, “Delegated content erasure in IPFS,” *Future Generation Computer Systems*, vol. 112, pp. 956–964, 2020.
[16] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, 2016, pp. 1–6.
[17] K. Kiania, S. M. Jameii, and A. M. Rahmani, “Blockchain-based privacy and security preserving in electronic health: a systematic review,” *Multimed. Tools Appl.*, vol. 82, no. 18, pp. 1–27, Feb. 2023.
[18] F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, “Blockchain from the perspective of privacy and anonymisation: A systematic literature review,” *Sensors (Basel)*, vol. 20, no. 24, p. 7171, Dec. 2020.
[19] H. D. Zubaydi, P. Varga, and S. Molnár, “Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review,” *Sensors (Basel)*, vol. 23, no. 2, p. 788, Jan. 2023.
[20] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.
[21] R. Belen-Saglam, E. Altuncu, Y. Lu, and S. Li, “A systematic literature review of the tension between the GDPR and public blockchain systems,” *Blockchain: Research and Applications*, vol. 4, no. 2, p. 100129, Jun. 2023.
[22] B. A. Kitchenham and S. Charters, “Guidelines for Performing Systematic Literature Reviews in Software Engineering,” EBSE Technical Report, Keele University and Durham University, 2007.
[23] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering,” in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, London, England, United Kingdom, 2014, pp. 1–10.
[24] W. Yánez, R. Bahsoon, Y. Zhang, and R. Kazman, “Architecting Internet of things systems with blockchain: A catalog of tactics,” *ACM Trans. Softw. Eng. Methodol.*, vol. 30, no. 3, pp. 1–46, Jul. 2021.
[25] L. Yang *et al.*, “Quality Assessment in Systematic Literature Reviews: A Software Engineering Perspective,” *Information and Software Technology*, vol. 130, p. 106397, 2021.
[26] S. Alsubai, A. Alqahtani, H. Garg, M. Sha, and A. Gumaei, “A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records,” *Complex Intell. Syst.*, vol. 10, no. 5, pp. 6117–6141, Oct. 2024.
[27] C. Daudén-Esmel, J. Castellà-Roca, and A. Viejo, “Blockchain-based access control system for efficient and GDPR-compliant personal data management,” *Computer Communications*, vol. 214, pp. 67–87, 2024.
[28] L. Yang *et al.*, “An access control model based on blockchain master-sidechain collaboration,” *Cluster Comput*, vol. 27, no. 1, pp. 477–497, Feb. 2024.
[29] S. Datta and S. Namasudra, “Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing,” *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4026–4036, Feb. 2024.

[30] L. Dong, J. Zhao, T. Chen, Y. Yu, Z. Duan, and J. Zhu, "The secure data sharing and interchange model based on blockchain for single window in trade facilitation," in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, Huaihua City, China, 2022.
[31] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed Vehicular Networks," *Appl. Sci. (Basel)*, vol. 10, no. 6, p. 2011, Mar. 2020.
[32] Y.-L. Lee, H.-A. Lee, C.-Y. Hsu, H.-H. Kung, and H.-W. Chiu, "SEMRES - A Triple Security Protected Blockchain Based Medical Record Structure," *Computer Methods and Programs in Biomedicine*, vol. 215, Mar. 2022.
[33] S. Luo, N. Han, T. Hu, and Y. Qian, "Secure Sharing of Electronic Medical Records Based on Blockchain," *International Journal of Distributed Sensor Networks*, vol. 2024, no. 1, p. 5569121, 2024.
[34] M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji, and A. AlGhuwainem, "MedAccess: A Scalable Architecture for Blockchain-based Health Record Management," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2020, pp. 1–5.
[35] S. Parthasarathy, A. Harikrishnan, G. Narayanan, L. J., and K. Singh, "Secure distributed medical record storage using blockchain and emergency sharing using multi-party computation," in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 2021, pp. 1–5.
[36] K. Sha, K.-B. Yue, W. Wei, Y. Wu, M. Koduru, and P. Vuchuru, "ConsortiumSec: Blockchain-based distributed security framework for consortium applications," *Distrib. Ledger Technol.*, Oct. 2024.
[37] H. Bodur and I. F. T. Al Yaseen, "An Improved blockchain-based secure medical record sharing scheme," *Cluster Comput.*, vol 29, no. 6, Apr. 2024.
[38] C. Hu *et al.*, "CrowdMed-II: a blockchain-based framework for efficient consent management in health data sharing," *World Wide Web*, vol. 25, no. 3, pp. 1489–1515, May 2022.
[39] Z. Liu, A. Yang, H. Zeng, C. Jiang, and L. Ma, "A Generalized Blockchain-Based Government Data Sharing Protocol," *Security and Communication Networks*, vol. 2023, pp. 1–9, Feb. 2023.
[40] M. Shah, C. Li, M. Sheng, Y. Zhang, and C. Xing, "Smarter Smart Contracts: Efficient Consent Management in Health Data Sharing," *Lect. Notes Comput. Sci.*, vol. 12318 LNCS, pp. 141–155, 2020.
[41] H. Wu, Y. Shang, L. Wang, L. Shi, K. Jiang, and J. Dong, "A Patient-Centric Interoperable Framework for Health Information Exchange via Blockchain," in *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*, Xi'an, China, 2020, pp. 76–80.
[42] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, "The case of HyperLedger Fabric as a blockchain solution for healthcare applications," *Blockchain: Research and Applications*, vol. 2, no. 1, p. 100012, Mar. 2021.
[43] Y. Dai, G. Lu, and Y. Huang, "A Blockchain-Based Access Control System for Secure and Efficient Hazardous Material Supply Chains," *Mathematics*, vol. 12, no. 17, p. 2702, Aug. 2024.
[44] Y. Dong, Y. Li, Y. Cheng, and D. Yu, "Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption," *High-Confidence Computing*, vol. 4, no. 1, p. 100168, 2024.
[45] K. Gai, Y. She, L. Zhu, K.-K. R. Choo, and Z. Wan, "A Blockchain-Based Access Control Scheme for Zero Trust Cross-Organizational Data Sharing," *ACM Trans. Internet Technol.*, vol. 23, no. 3, Aug. 2023.
[46] D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for Industrial IoTs," *Pervasive and Mobile Computing*, vol. 88, p. 101738, 2023.
[47] J. Hu, P. Zhu, J. Li, Y. Qi, Y. Xia, and F.-Y. Wang, "A secure medical information storage and sharing method based on multiblockchain architecture," *IEEE Trans. Comput. Soc. Syst.*, vol. 11, no. 5, pp. 6392–6406, Oct. 2024.
[48] Y.-T. Lei, C.-Q. Ma, N. Mirza, Y.-S. Ren, S. W. Narayan, and X.-Q. Chen, "A renewable energy microgrids trading management platform based on permissioned blockchain," *Energy Economics*, vol. 115, p. 106375, 2022.
[49] J. Li, D. Han, Z. Wu, J. Wang, K.-C. Li, and A. Castiglione, "A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control," *Future Gener. Comput. Syst.*, vol. 142, pp. 195–211, May 2023.
[50] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Computers and Electrical Engineering*, vol. 103, p. 108379, 2022.
[51] Q. Wang and Y. Liu, "Enhancing Collaborative Emergency Management: Leveraging Blockchain Distributed Ledger for Inter-Agency Data Sharing," in *Proceedings of the 8th ACM SIGSPATIAL International Workshop on Security Response Using GIS*, Hamburg, Germany, 2023, pp. 13–17.
[52] Y. Wang, C. Li, P. Li, B. Feng, and Z. Li, "Research on trusted sharing method of railway spatiotemporal data based on blockchain technology," in *Proceedings of the International Conference on Algorithms, Software Engineering, and Network Security*, Nanchang, China, 2024, pp. 157–163.
[53] Y. Wang and A. Kogan, "Designing confidentiality-preserving Blockchain-based transaction processing systems," *International Journal of Accounting Information Systems*, vol. 30, pp. 1–18, Sep. 2018.

[54] F. Yu *et al.*, “Research on Multi-Blockchain Electronic Archives Sharing Model,” *Computers, Materials and Continua*, vol. 76, no. 3, pp. 3921–3931, 2023.
[55] Y. Zheng, Z. Cheng, Y. Liu, B. Wang, and C. Zhu, “Collaborative Learning for Cross-Organizational Data Sharing Using Hyperledger Fabric,” 2023, pp. 285–292.
[56] Z. Chen, “Enhancing the engineering supervision process in China: A solution enabled by integrating hybrid blockchain system,” *Innovation and Green Development*, vol. 2, no. 4, p. 100091, 2023.
[57] Y. Hou, M. Luo, Y. Liu, N. Wang, J. Zhang, and W. Xu, “Secure and Privacy-Preserving Data Computing Scheme Based on Blockchain for Double-Loop Governance of Smart Society,” in *Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications*, Xi’an, China, 2021, pp. 75–80.
[58] W. Li, W. K. Tse, and J. Chen, “Privacy and security mechanisms for B2B data sharing: A conceptual framework,” *Information (Basel)*, vol. 15, no. 6, p. 308, May 2024.
[59] H. Si *et al.*, “A cross-chain access control mechanism based on blockchain and the threshold Paillier cryptosystem,” *Computer Communications*, vol. 223, pp. 68–80, 2024.
[60] C. Gupta, V. Gupta, and J. M. Fernandez-Crehuet, “A blockchain-enabled solution to improve intra-inter organizational innovation processes in software small medium enterprises,” *Engineering Reports*, vol. 5, no. 7, Jul. 2023.
[61] J. Lin *et al.*, “FGDB-MLPP: A fine-grained data-sharing scheme with blockchain based on multi-level privacy protection,” *IET Communications*, vol. 18, no. 4, pp. 309–321, 2024.
[62] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, “HealthBlock: A secure blockchain-based healthcare data management system,” *Comput. Netw.*, vol. 200, no. 108500, p. 108500, Dec. 2021.
[63] X. Jia *et al.*, “Cross-organisational data sharing framework based on blockchain-probes,” *IET Networks*, vol. 12, no. 2, pp. 77–85, 2023.
[64] Y. Lin *et al.*, “Power data blockchain sharing scheme based on homomorphic encryption,” in *2022 IEEE 5th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Chongqing, China, 2022.
[65] S.-J. Hsiao and W.-T. Sung, “Blockchain-based supply chain information sharing mechanism,” *IEEE Access*, vol. 10, pp. 78875–78886, 2022.
[66] M. A. Habib, K. Md. Rokibul Alam, and Y. Morimoto, “A secure medical record sharing scheme based on blockchain and two-fold encryption,” in *2022 25th International Conference on Computer and Information Technology (ICCIT)*, Cox’s Bazar, Bangladesh, 2022, pp. 78–83.
[67] Y.-S. Ren, C. Ma, and Y. Wang, “A new financial regulatory framework for digital finance: Inspired by CBDC,” *Global Finance Journal*, vol. 62, p. 101025, 2024.
[68] Q. Wang, H. Dong, Y. Huang, Z. Liu, and Y. Gou, “Blockchain-Enabled Federated Learning for Privacy-Preserving Non-IID Data Sharing in Industrial Internet,” *Computers, Materials and Continua*, vol. 80, no. 2, pp. 1967–1983, 2024.
[69] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, “A blockchain-based medical data sharing and protection scheme,” *IEEE Access*, vol. 7, pp. 118943–118953, 2019.
[70] S. Wu and J. Du, “Electronic medical record security sharing model based on blockchain,” in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, Kuala Lumpur, Malaysia, 2019, pp. 13–17.
[71] X. Fang and M. Li, “Privacy-Preserving Process Mining: A Blockchain-Based Privacy-Aware Reversible Shared Image Approach,” *Applied Artificial Intelligence*, vol. 38, no. 1, p. 2321556, 2024.
[72] Akshaya, S. K. Shetty, and A. P. Patil, “Preserving and sharing of medical data using blockchain technology,” in *2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, Vijaypur, India, 2022, pp. 1–5.
[73] M. Xie, Q. Fu, H. Hong, Z. Ren, Z. Zhang, and J. Kuai, “ABBDAC: A Novel Attribute-Based Blockchain Data Access Control Scheme in Cloud Environment,” *IEEE Internet of Things Journal*, pp. 1–1, 2024.
[74] X. Zhang, Y. Su, J. Qin, and J. Sun, “SDTA: Secure Decentralized Trading Alliance for electronic medical data,” *Comput. Law J.*, vol. 67, pp. 2573–2585, Mar. 2024.
[75] H. Liang, Y. Guo, and K. Gai, “A blockchain-based hierarchical storage method for supply chain data,” in 2023 IEEE 8th International Conference on Smart Cloud (SmartCloud), Tokyo, Japan, 2023, pp. 105–110.