computers

MDPI

Article

Intelligent Attack Detection in Blockchain-Enabled Multi-Cloud Systems: A Systematic Review and SOC-LLM-Augmented Architecture Proposal

Adam Koty Abbass Ahmat * and Habiba Chaoui *

National School of Applied Sciences (ENSA), Ibn Tofail University, Kenitra 14000, Morocco
* Correspondence: adamkoty.abbassahmat@uit.ac.ma (A.K.A.A.); habiba.chaoui@uit.ac.ma (H.C.)

Abstract

This paper presents a systematic literature review examining how blockchain technologies can enhance the security and performance of multi-cloud systems. Multi-cloud architectures offer resilience, scalability, and flexibility; however, they also pose complex security challenges related to APIs, service-level agreements (SLAs), orchestration, and authentication. The promise of blockchain technology to improve the security and transparency of numerous applications, including cloud storage systems, has attracted considerable attention in recent years. Much research has focused on decentralized storage in cloud environments, spanning supply chains, FinTech, healthcare, and education. Still, the integration of blockchain with the cloud and its potential to enhance security and performance warrant an in-depth study. Using the PRISMA methodology, a structured search was conducted across six major scientific databases, including IEEE, ACM Digital Library, ScienceDirect, Scopus, Web of Science, and IJIMAI. Twenty-four primary papers published between 2019 and 2025 were selected for analysis after clear inclusion and exclusion criteria were applied. This review examines the security dimensions in multi-cloud environments—architectural vulnerabilities, API security, authentication, orchestration and automation vulnerabilities, SLAs, and cybersecurity compliance issues—in relation to blockchain technology. Based on the identified gaps, we propose a SOC-LLM-augmented security architecture that integrates blockchain-based evidence integrity, statistical anomaly detection, machine learning, large language models, and autonomous AI agents to enable intelligent attack detection and response. The proposed framework introduces specialized agents for detection, correlation, threat intelligence retrieval, blockchain evidence validation, explanation generation, and response planning. The analysis shows that integrating SOC-LLM capabilities with blockchain can move multi-cloud security from passive auditability toward proactive, explainable, and human-in-the-loop cyber defense. Finally, this paper discusses open challenges, including LLM hallucination, data scarcity, real-time scalability, evaluation standardization, and trustworthy deployment in critical multi-cloud infrastructures. The study's conclusion highlights research gaps and suggests future lines of inquiry concerning scalable blockchain architectures and the incorporation of AI for proactive cloud security monitoring.

Keywords: systematic review; multi-cloud security; blockchain; augmented SOC; sophisticated attack; LLM

Check for updates

Academic Editor: Paolo Bellavista

Received: 9 June 2026
Revised: 28 June 2026
Accepted: 8 July 2026
Published: 17 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

With their interpretations of the Internet as a central service provider, blockchain technology and the cloud have drawn the interest of numerous enterprises in recent years. Although many apps generate a significant amount of data, they require storage space to leverage blockchain technology [1]. Cloud storage systems offer a variety of storage services to satisfy organizational requirements—namely, for dynamic data storage, service capacity, and cloud service providers' prices. Instead of building and maintaining internal storage networks, using these storage services can result in cost savings. Data owners may externalize their data to the cloud and use an unlimited resource by paying cloud service providers (CSPs).

Numerous studies have been conducted on cloud system security. When users entrust CSPs with their data, they provide them access, which implies that the user has limited control over what happens to the data [2]. According to [3], many security and performance issues have been resolved by implementing data integrity auditing for CSPs.

The primary issue associated with data loss is CSPs' ability to conceal mistakes made with user data to benefit from it [4]. Because of its high level of security, decentralized data storage is advantageous for data integrity and confidentiality [5]. Data is separated into blocks and encrypted using hashes or public–private key pairs. The blockchain technology itself is safe, and any malevolent users or bad actors cannot access the entire process [6]. Decentralized data storage has several benefits, including increased dependability, reduced costs, and security [7,8], as well as the use of P2P networks.

Since distributed file storage solutions are based on blockchain technology, there is no trust in controlling the network. As a result, these storage techniques offer greater security than others. Because encrypted files must be repeatedly decrypted and re-encrypted, security issues may also occur if the data is altered or shared with a third party [9].

Additionally, data distribution over a network is not safe; it is only secure when the data is kept up to date. With a private blockchain, the network can be customized to meet specific requirements, such as the rate at which data is stored or the encryption method used within the blockchain.

Although system security and performance present significant issues, multi-cloud systems are increasingly indispensable in an era of technological progress, adaptability, scalability, and resilience. The protection of data and services is made more difficult by recognized security dimensions, including architecture, APIs, authentication, orchestration and automation, service level agreement (SLA) management, and cybersecurity rules. Blockchain technology offers promising opportunities and can be integrated into these systems to address the six vectors mentioned. Nonetheless, it is crucial to conduct a thorough analysis of the security needs and specific risks associated with various attack methods.

This research initially presents a systematic review of six blockchain-based security dimensions to ensure integrity, confidentiality, modification, and third-party sharing in multi-cloud systems, covering the 2019–2025 period. Based on our investigation and analysis, this study proposes a security framework augmented with SOC-LLM for blockchain-enabled multi-cloud systems. It begins by reviewing current blockchain-based solutions based on six security dimensions: architecture, API security, authentication, orchestration and automation, SLA management, and cybersecurity compliance. Then it lists the major limitations, such as limited proactive attack detection, no uniform evaluation, and issues with scalability and interoperability. The report proposes a reference architecture that combines statistical anomaly detection, machine learning, multi-agent LLM reasoning, SIEM/SOAR workflows, RAG-based threat intelligence, and blockchain-based evidence management to

fill these gaps. The work ends with identifying promising research directions for deploying SOC-LLMs that are reliable, explainable, scalable, and human-in-the-loop.

The remainder of this paper is structured as follows: Section 2 presents the background; Section 3 reviews prior research on multi-cloud, blockchain, and multi-cloud storage security. Section 4 explains the research methodology. Section 5 presents the analysis results and discussion. Section 6 proposes a novel SOC-LLM architecture. Finally, Section 7 presents the conclusion and directions for future work.

2. Background

2.1. Integration of Blockchain in a Multi-Cloud System

The combination of blockchain and multi-cloud technology represents a substantial shift in the state of the art. Although integrating blockchain technology into multi-cloud management offers several benefits in security, transparency, and cost-effectiveness, the process is complex. The complexity of this integration stems from issues such as integrating blockchain into an existing multi-cloud infrastructure, the possibility of distinct standards and protocols among cloud service providers, and the difficulty of ensuring interoperability between various blockchain platforms and cloud providers.

Hyperledger Fabric was our choice because it meets our objectives and provides a certified, trusted, and secure blockchain infrastructure for creating decentralized apps. Several organizations use it because of its qualities; it is a suitable option for developing decentralized applications at the corporate level. It has several characteristics that make it appropriate for blockchain applications at the corporate level [9], including: modular architecture, an authorized network, smart contracts, a consensus mechanism, and privacy and confidentiality.

2.2. Blockchain and IAM

Access models are a fundamental component of IAM systems, which ensure that only authorized individuals have access to sensitive information and systems. IAM solutions are required to guarantee data and resource security. They ensure that only verified identities have access to system data assets and manage the lifecycle of digital identities. The two primary functions of the IAM system, AuthZ and AuthN, control access to data and verify identity, respectively [10]. Different models and standards for access control and access management can be used to implement AuthZ and AuthN.

IAM systems play a critical role in controlling access to resources across cloud instances. However, typical centralized IAM systems face challenges with scalability, data security, and performance overhead [11]. We will use blockchain technology in the IAM system to overcome these issues. Two blockchain-based IAM architectures have been proposed: self-sovereign identity (SSI) and decentralized trusted identity [12]. These approaches are designed to provide safe, decentralized, and user-controlled identities for people and objects in the digital world. IAM systems strive to offer safe, scalable identity management solutions that protect privacy by leveraging cutting-edge technologies such as blockchain.

The five categories of access control determine how users can access data in IAM. These models form the basis for granting authorizations to identities or users based on their required responsibilities and attributes. Many access management standards, including OpenID Connect, markup languages for open authorization, security assertions, and flexible access control, are used to satisfy the access control procedures for AuthZ and AuthN [13]. Many IAM systems have been proposed using BC, based on the Self-Governed Identity (SSI) and Decentralized Trusted Identity IAM models [14].

2.3. SOC-LLM and Agentic Threat Detection

Modern security operations centers (SOCs) rely on SIEM and SOAR platforms to collect security events, correlate alerts, and support incident response. However, multi-cloud environments generate high-volume, heterogeneous data from APIs, IAM services, orchestration layers, network flows, SLA metrics, and blockchain events. This complexity makes traditional rule-based monitoring ineffective at detecting intelligent, distributed, and evolving attacks. Therefore, combining statistical anomaly detection, machine learning, and LLM-based reasoning can enhance SOCs' ability to detect anomalous behavior, correlate weak signals, and provide contextual explanations for security analysts.

In this study, SOC-LLM is positioned as an intelligent security layer that complements blockchain-based trust in multi-cloud systems. Blockchain provides integrity, traceability, and tamper-resistant evidence. At the same time, the SOC-LLM layer enables proactive threat detection through multi-agent reasoning, retrieval-augmented threat intelligence, and human-in-the-loop validation. Specialized agents support alert classification, anomaly correlation, blockchain evidence validation, attack explanation, and response planning. The goal of this integration is to shift multi-cloud security from passive auditing to proactive, explainable, and adaptive cyber defense.

2.4. LLMs in Cybersecurity: Recent Advances and Relevance to SOC Operations

2.4.1. AI-Assisted SOC Operations and Security Copilots

By automating alarm triage, generating plain-language incident descriptions, and suggesting containment actions, LLMs can dramatically reduce analyst burden, according to recent work on AI-assisted SOC operations. Fine-tuned LLMs can outperform rule-based systems at identifying complex, multi-step attack narratives from heterogeneous SIEM logs, as shown in studies such as [15]. The SOC-LLM Detection and Explanation Agent functions specified in our design are empirically grounded by this body of work.

The first commercial implementations of LLMs integrated into business SOC procedures appear in security copilot systems, namely IBM's AI for Cybersecurity platform and Microsoft Security Copilot. These tools provide analysts with automated attack mapping, guided remediation playbooks, and natural-language querying of threat intelligence using GPT-4-class models. They validate the core concept of our SOC-LLM layer while preserving confidentiality. Crucially, these systems lack multi-agent supervision methods and blockchain-based proof integrity, which we view as the key differentiators of our proposed design.

2.4.2. Agent-Based Security Architectures and Retrieval-Augmented Security Analysis

Cybersecurity research has examined multi-agent LLM architectures; frameworks such as [16,17] demonstrate the potential of cooperative autonomous agents for offensive security tasks. On the defensive side, agent-based SOAR process automation has been explored by Auto-Defense and related systems. By assigning each agent a specific cybersecurity role and adding a hierarchical supervisory agent to prevent unchecked autonomous decision-making, a governance mechanism notably lacking in most existing agent-based security systems, our suggested architecture builds on this paradigm.

In high-stakes security scenarios, Retrieval-Augmented Generation (RAG) has become a crucial method for eliminating hallucinations and firmly grounding LLM-based security analysis in verified threat data. RAG pipelines that Champ use index CVE databases, MITRE attack databases, and operational playbooks [18] and related systems to provide context-anchored suggestions. This directly shapes the architecture of our RAG Threat Intelligence Agent, in which the retrieval corpus comprises internal reaction playbooks, MITRE-like databases, and vulnerability documentation. The proposed integration of RAG

with blockchain-verified evidence chains is a unique architectural contribution that has not been discussed in prior research.

3. Related Works

Many organizations, including those in the financial, medical, and governmental sectors, are adopting multi-cloud technology because it has proven advantageous. However, security remains a problem today.

Because the cloud is scalable and relatively cost-effective, many businesses seeking flexible access to IT resources, such as servers, storage, databases, and software applications, opt for it [19]. However, the cloud also poses several security challenges, including identity theft and data breaches, that threaten the confidentiality, integrity, and availability of cloud-based systems and data.

As shown in ref. [20], HSE has shown that using multiple providers can help distribute workloads and avoid service interruptions in the event of a cloud provider failure or outage. Numerous studies have examined cloud security, and to ensure platform confidentiality, integrity, and availability, the National Institute of Standards and Technology (NIST) has outlined best practices for safeguarding cloud-based systems and data. These include strict access controls, data encryption, and continuous monitoring of the cloud environment.

In multi-cloud settings, blockchain has been explored in prior research for auditing cloud systems [21] to mitigate data auditing challenges. A PDP protocol was proposed to protect user privacy during public auditing by enabling auditing of public data through trustworthy TPAs.

Several ideas have been proposed to improve blockchain-based storage networks. By storing zone file hashes, researchers in [22] have developed a decentralized, blockchain-based Domain Name System (DNS) to prevent data manipulation. To avoid collapse if one of the nodes fails, it also has many parallel analysis nodes. Private blockchains store each file's metadata, while Distributed Hash Tables (DHTs) store the actual files off-chain. Blockchain-based storage networks use private blockchains to generate revenue from idle storage capacity. Redundancy and data availability are examined at predetermined intervals. Dual smart contracts oversee logging, payment, and storage security within this network.

Table 1 presents suggested methods to enhance the security of current blockchain-based storage networks and to ensure data security and access management. In most prior research, blockchain has been used to ensure data security in the cloud and to secure access to cloud resources.

Table 1. Research on IAM and decentralized storage networks based on blockchain.

Paper Type	Title	Major Contribution	Features Research Directions	Year	Reference
Research	Bi-Quad Merkle Tree-Based Blockchain-Based Approach to Protect Job Card Data Integrity and Payment System	Suggested a methodology to protect data using the RSA and DES (MRDES) encryption algorithm while lowering the compute cost and temporal complexity of the transactions management process.	Add lightweight cryptography based on block contents to the model to further improve resilience against security risks and further minimize complexity.	2024	[23]
Review	Identity Management, SSI and Blockchain: A Review	integration and combination of blockchain technology and Facial Recognition Technology (FRT) in Self-sovereign identity (SSI) to ensure identity performance and security.	Using SSI to drive a biometric revolution that goes beyond conventional identity management, providing a simple and safe authentication procedure across a range of industries. Accessing government services, medical records, or financial transactions is made faster and more secure when Facial Recognition Technology is connected with SSI.	2023	[24]

Table 1. *Cont.*

Paper Type	Title	Major Contribution	Features Research Directions	Year	Reference
Research	Using Hierarchical Data Protection with Brotli Compression to Provide Safe and Effective Multi-Cloud Storage.	A system that utilizes the MD5 algorithm and the Brotli compression method is suggested to guarantee data integrity, minimize data size, and facilitate speedier transmission.	For cold files that don't require frequent read–write operations, the suggested approach works better. This, if the files needed read–write operations, is the performance accuracy.	2023	[1]
Survey	Blockchain-Based Identity Management Systems in Health Iot: A Systematic Review.	A systematic literature review on the blockchain-based IAM in Health IOT. They compared 24 studies in terms of IAM based on blockchain in Health IOT.	The creation of an all-encompassing security framework for Internet of Things applications using BC-based IAM systems.	2022	[25]
Research	Decentralized Storage Network	It has suggested a method for effectively regulating the storage agreement between the customer and storage provider by utilizing the Oracle network and smart contracts.	The legitimacy of the outcome can be increased by using the Oracle network and smart contract to control the storage contract regulations.	2022	[26]
Review	Blockchain-Based Secure Storage	To increase the security of communication transactions, an information compression technique based on double blockchains was presented for stored data.	When using the RSA and DSA algorithms, the accuracy of the suggested system can reach 96%.	2021	[27]

4. Research Methodology

By merging blockchain technology with related subjects in the literature, it is necessary to examine the numerous challenges posed by cloud security and analyze prior work.

This study employs a multidisciplinary framework and adheres to PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) criteria. The aim is to identify studies on the security of multi-cloud systems that integrate blockchain in response to the six identified attack vectors, as well as future directions in this area. Accordingly, we have identified and collated all relevant literature in which blockchain has been used to address the six security dimensions: architecture, APIs, authentication, multi-cloud automation and orchestration, SLA, and cybersecurity legislation. The planning, implementation, and reporting phases encompass the three primary stages of the review. Finally, an exploratory study is conducted to assess the current state of blockchain technology deployment in decentralized storage. All the literature has been compiled to identify current research topics and unanswered questions.

4.1. Research Question

We established the following primary research questions to guide our systematic analysis:

(1) What advantages may the integration of blockchain technology provide to a multi-cloud system?
(2) How can the six newly discovered security dimensions be addressed with blockchain technology?
(3) Can blockchain technology be integrated with other technologies to address the six security threat vectors in multi-cloud environments?
(4) How can the blockchain-based multi-cloud system be effectively safeguarded against the six security dimensions outlined in this article?
(5) What advantages can we gain from modern technology to successfully address these challenges?

An essential component of any systematic literature review is the development of the search methodology. The research protocol outlines procedures for identifying relevant research, including selecting databases to search, selecting search terms and inclusion/exclusion criteria, selecting pertinent studies, and evaluating their quality. The selected papers are shown in Table 2.

Table 2. Population, Intervention, Comparison, and Outcome (PICO) criteria used in this study.

Exclusion Criteria	Inclusion Criteria
- Studies that are not written in English - Research released before 2019 - Duplicate publications and secondary research - Multi-cloud apps, rather than blockchain, serve as the foundation for cloud systems - Not related to blockchain integration in cloud systems	- Studies written in English - Research works released in 2019–2025 - peer-reviewed - publications or original research on multi-cloud blockchain systems - proposed blockchain-based approaches applied to cloud or multi-cloud systems, - addressed security or performance challenges

4.2. Identification of Research

4.2.1. Sources of Research

Table 3 lists the six databases selected for analysis to identify all studies relevant to our research concerns. These databases were found to cover all published research on the security of the six (6) security dimensions listed below, as well as on the integration of blockchain technology in cloud and multi-cloud environments. The databases were selected based on research topics in computer technology and emerging technologies. Articles were sorted by publication date from 2019 to 2025.

Table 3. Databases utilized in the comprehensive analysis.

Database	Website
ACM	https://www.acm.org/ (accessed on 15 May 2024)
IEEE	https://ieeexplore.ieee.org/ (accessed on 15 May 2024)
IJIMAI	https://www.ijimai.org/journal/ (accessed on 15 May 2024)
Science Direct	https://www.sciencedirect.com/ (accessed on 15 May 2024)
Scopus	https://www.scopus.com/pages/home (accessed on 15 May 2024)
Web of Science	https://webofscience.com/ (accessed on 15 May 2024)

4.2.2. Criteria Selection

Cloud, blockchain, and security were initially considered important terms. Later, six more keywords were added to the original list, including architecture, API, IAM, multi-cloud automation and orchestration, SLA, and cybersecurity laws. Additionally, two more keywords were proposed for the IAM section: identity and authentication.

To ensure that only pertinent primary studies were selected, the article selection criteria were based first on relevance and then on the article selection date, which falls between 2019 and 2025. Every study on the final list satisfied these requirements, and the inclusion and exclusion criteria are shown in Table 4.

Table 4. Criteria for inclusion and exclusion.

Criteria	The Equivalent
Population	- Blockchain, cloud & security.
Action	- Security based on Blockchain systems with many clouds. - Various approaches to integrating blockchain technology into a multi-cloud system while keeping an eye on the six vectors.
Evaluation	- Protection, security, and confidentiality of the blockchain-powered multi-cloud systems. - Increasing the multi-cloud blockchain-based systems' dependability.
Results	

4.2.3. Research Strategy

A systematic search was conducted across the following scientific databases: ACM, IEEE, IJIMAI, ScienceDirect, Scopus, and Web of Science. The search queries combined keywords for blockchain, cloud computing, and security mechanisms.

The terms "cloud," "multi-cloud," and "blockchain" were once considered the most important search terms. Synonyms for keywords and related concepts were then defined. Subsequently, the keywords of each of the six identified vectors—"architecture," "API," "authentication," "orchestration," "cybersecurity"—were used in conjunction with the phrase "blockchain." Terms such as IAM, authentication, and authorization were added to the keyword list for the authentication section because they were used in our search. Our research synthesis focuses on blockchain and cloud computing. As a result, the search was also prioritized by publication date for each search category. The following keywords and their synonyms were included in our research process: Blockchain, cloud, multi-cloud, architecture, API, IAM, authentication, authorization, orchestration, cybersecurity, and SLA.

To maximize the search's scope while preserving its relevance, synonyms and related terms were used whenever the relevant databases permitted. Without changing the question's semantic meaning, the search technique was slightly modified to satisfy the syntactic specifications of each digital library. However, after identifying pertinent, comparable papers that complemented our study's goal, the six databases mentioned or selected in this article were chosen.

4.2.4. Selection Process and Exclusion Criteria for Relevant Studies

The PRISMA standards for the article selection flowchart are explained in detail through the processes shown in Figure 1.

These procedures were used to select relevant research. Using Zotero, relevant studies were first added to a group for each database. After that, to eliminate duplicates, they were categorized by keyword in a library.

In total, 1283 records were initially identified. Inclusion and exclusion criteria were applied. Based on reference categories and duplicate research, 296 entries were excluded by perimeter exclusion. A total of 921 papers were eliminated based on the title, abstract, and the date of the research that was chosen. Out-of-scope and secondary studies were eliminated. The final stage involved downloading and reading the remaining 66 papers to evaluate their quality and inclusion/exclusion, and to apply quality assessment criteria.

To ensure transparency and reproducibility, the research selection procedure followed three steps and was based on the PRISMA 2020 recommendations. A total of 1283 references were obtained from the six selected scientific databases during the identification phase. Zotero was used to identify and remove duplicate publications. The remaining references were excluded because they were editorials, book chapters, unfinished articles, or publications that did not meet the predetermined inclusion criteria. During the pre-selection phase, the titles and abstracts of the remaining papers were compared against the predetermined inclusion and exclusion criteria. Studies not written in English, published before 2019, unrelated to blockchain-based cloud or multi-cloud systems, or on conventional cloud computing without blockchain integration, as well as secondary studies such as literature reviews, surveys, tutorials, or opinion pieces, were excluded. The final eligibility process consisted of evaluating the full texts of the remaining studies. Articles that did not cover at least one of the designated security areas, did not provide sufficient technical information, or did not propose or assess blockchain-based solutions suitable for cloud or multi-cloud systems were eliminated.

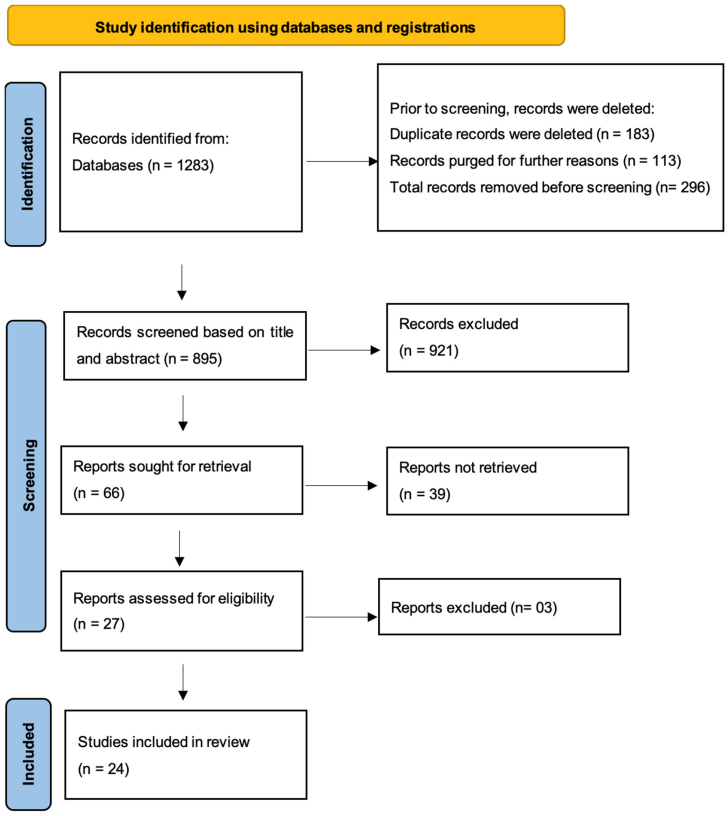

Figure 1. Article selection steps.

The four stages of our PRISMA process selection for this study are summarized below:

- Identification: 1283 articles were initially identified through database searches.
- Screening: After removing 296 duplicate articles, the titles and abstracts of the remaining 987 articles were screened.
- Eligibility: 66 articles were selected for full-text review.
- Inclusion: 24 studies met all criteria and were included in the final analysis.

4.2.5. Study Selection and Quality Assessment

Ref. [28] asserts that quality evaluation is essential to removing bias in chosen research. To guarantee that every main study met the research topics, the quality evaluation criteria listed in Table 5 were applied. Achieving a quality score of 1.0 for each checklist criterion is required to pass the quality evaluation. The research was deemed ineligible if it did not achieve a quality score of 1.0 across all quality evaluation parameters. Excluded from consideration were theoretical and incomplete research, as well as studies that failed to consider blockchain technology. Furthermore, papers that omitted any of the important vector phrases identified in our search were excluded.

According to the PRISMA approach, the study selection process comprised four steps: identification, selection, eligibility assessment, and inclusion. All identified documents were collected. Duplicates were removed using the bibliographic management program Zotero. Titles and abstracts were then screened against predetermined inclusion and exclusion criteria. Only peer-reviewed research on blockchain applications in cloud or multi-cloud systems, published in English between 2019 and 2025, was considered. Articles outside the study's scope, secondary research, duplicate publications, and studies unrelated to blockchain integration were excluded. The remaining publications underwent full-text analysis to verify their applicability to at least one of the six specified security domains and their contribution to cloud security through blockchain.

Table 5. Quality assessment criteria.

The Factor for Evaluating the Quality	Yes	No
Is the research question addressed in the study?	1	0
Is the cloud system implemented using a blockchain platform?	1	0
Is the security of the system considered?	1	0

Each eligible study underwent an additional evaluation using a quality assessment grid with three criteria to ensure methodological rigor: (i) the study's explicit address of the research questions; (ii) the implementation of blockchain in a cloud or multi-cloud environment; and (iii) a thorough analysis of security aspects. Each criterion was scored as 1 (Yes) or 0 (No), and only studies that met all quality requirements were included in the final synthesis. This quality evaluation improves the systematic review's dependability and reduces the likelihood of including research that is speculative, incomplete, or flawed.

In total, 24 studies were selected by this procedure and considered for further analysis and discussion.

5. Results and Discussion

Table 6 presents the final collection, comprising 24 peer-reviewed studies selected after applying the inclusion, exclusion, and quality assessment criteria. To address the three primary research concerns, research gaps and future directions were identified based on the total number of retrieved records. However, some omitted studies appeared to meet the inclusion criteria; they were excluded either because they did not integrate security considerations into the system or because they were not relevant to the overall analysis.

Table 6. Final list of included studies.

Study	Title	Authors Names	Type	Year	Publisher	References
S1	Blockchain-based Solution for Securing Job Card Data Integrity and Payment System using Bi-Quad Merkle Tree	Sabeena and Vijila	Journal Article IJISAE	2024	Elsevier	[23]
S2	EXPLOITING AI AND SOURCE BLOCKCHAIN FRAMEWORK TO MITIGATE RISKS IN CLOUD MANUFACTURING IN INDUSTRY3.0	Gangadhara	Journal Article ijmec	2021	ResearchGate	[29]
S3	Performance evaluation of Private and Public Blockchains for multi-cloud service federation	Zahir and al.	Conference paper	2024	ACM	[30]
S4	A Secure and Efficient Blockchain-based Multi-Cloud Medical File Sharing	SH and al.	Conference paper	2023	IEEE	[31]
S5	IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-based Approach Towards a Trustworthy Cloud Computing	Irshad and al.	Journal Article	2023	IEEE	[32]

Table 6. *Cont.*

Study	Title	Authors Names	Type	Year	Publisher	References
S6	An Efficient Integrity Verification based Multi-User Cloud Access Control Framework using Block Chain Technology on EHR Database	Sravanthi and Sekhar	Journal Article IJISAE	2024	Elsevier	[33]
S7	Enhancing the Trustworthiness of 6G Based on Trusted Multi-Cloud Infrastructure: A Practice of Cryptography Approach.	Zhou and al.	Journal Article	2024	CMES	[34]
S8	A blockchain-based cloud forensics architecture for privacy leakage prediction with cloud	Ragu and Ramamoorthy	Journal Article	2023	Science Direct	[35]
S9	Blockchain-Based Cloud Management Architecture for Maximum Availability	Arias Maestro and al.	Journal Article	2023	IJIMAI	[36]
S10	Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks	Zeydan and al.	Journal Article	2022	IEEE	[37]
S11	Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud	Wu and al.	Journal Article	2022	Science Direct	[38]
S12	Blockchain and API Development to Improve Relational Database Integrity and System Interoperability	Ramadhan and al.	Journal Article	2023	Science Direct	[39]
S13	Connect API with Blockchain: A Survey on Blockchain Oracle Implementation	Pasdar and al.	Journal Article	2023	ACM	[40]
S14	Permissioned Blockchain Reinforced API Platform for Data Management in IoT-based Sensor Networks	Baucas and Spachos	Conference Paper	2021	IEEE	[41]
S15	Security and standardization of a notary-based blockchain interoperability API	Scheid and al.	Conference Paper	2021	IEEE	[42]
S16	Blockchain-integrated decentralized fault tolerance for secure and energy-efficient multi-cloud interoperability	Sivagami, V.M. and al.	Journal Article	2025	Elseiver	[43]
S17	A Trustworthy Framework for Multi-Cloud Service Management: Self-Sovereign Identity Integration	Zeydan and al.	Journal Article	2024	IEEE	[44]
S18	An integrated architecture for maintaining security in cloud computing based on blockchain	Awadallah and al.	Journal Article	2021	IEEE	[45]
S19	Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain	Son and al.	Journal Article	2020	IEEE	[46]
S20	Continuous Compliance Model for Hybrid Multi-Cloud through Self-Service Orchestrator	Rompicharla	Conference Paper	2020	IEEE	[47]
S21	Towards a Secured IoT Communication: A Blockchain Implementation Through APIs	Verma and al.	Book Section	2023	Springer	[48]
S22	Blockchain-based automated container cloud security enhancement system	Sun and al.	Conference Paper	2020	IEEE	[49]

Table 6. *Cont.*

Study	Title	Authors Names	Type	Year	Publisher	References
S23	A Security-Enhanced Monitoring System for Northbound Interface in SDN using Blockchain	Hoang and al.	Conference Paper	2019	ACM	[50]
S24	Integration of Blockchain with AWS and Azure for Enhanced Cloud Security and Compliance in Multi-Cloud Architectures	Patil, Balkrishna	Conference Paper	2025	IEEE	[51]

The information extracted from it indicates that extensive research has been conducted and that there has been a recent surge in research on cloud security through blockchain integration. Research has indicated that architectural security, which focuses on identity recognition and data transaction protection on the cloud, is possible, but blockchain cannot safeguard the cloud system's design.

Out of the 24 entries, seven studies, representing approximately 29.2% of the corpus, addressed system security issues such as data integrity, confidentiality, and transparency while focusing on the viability and integration of blockchain technology with cloud services. Three studies integrated cloud orchestration; five examined the integration and use of blockchain with APIs in cloud systems; five focused on system design security; and one incorporated SLA security. Several studies on the shift from authentication to authorization across various systems were presented under the headings "IAM" or "authentication"; nevertheless, our article included three of them (which met the selection criteria). The inclusion of security and blockchain in our inclusion criteria poses a risk to the evaluation of the included research, particularly for IAM.

Ethereum and Hyperledger Fabric are the most widely used blockchain technologies, according to the data. Figure 2 shows that 50% of studies employed the Ethereum blockchain in their solutions, 45% used the Hyperledger Fabric blockchain as the foundation, and 5% used other blockchain platforms.

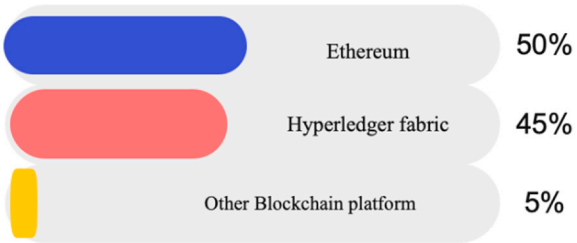

Figure 2. The Blockchain Technologies Used.

The results confirm that blockchain primarily supports decentralized access control, trust, traceability, and integrity; however, interoperability and scalability remain unresolved problems. Hyperledger and the corporate Ethereum Alliance, two of the most well-known corporate blockchain systems, have decided to collaborate to establish the standards required for interoperability (block–cloud integration). We will discuss the two main research topics in this part, each covered in a subsection.

The solutions found in the selected and reviewed research fall into six categories, which are further subdivided into six (6) blockchain-powered cloud system attack vectors.

Table 7 shows that S8–S11′s research focuses on the security of blockchain-based cloud system architecture; S12–S16′s research is more security-focused (but still blockchain-based) and examines the use of APIs to access cloud services; and S17–S19′s research integrates

AuthZ and AuthN while examining the security of blockchain-based IAM. The research focus of S20–S22 is blockchain security in cloud orchestration.

Table 7. Details of selected studies.

Study	Application	BC Platform	BC Type	Security Assets	Access Policy
S1	Job Cards Payments	Ethereum	Bi-Quad Merkle	integrity, privacy, confidentiality	permissioned
S2	Cloud manufacturing applications	Hyperledger Fabric	private	Data security, predictive auditing, risk management	Permissioned
S3	NFV MANO System	Ethereum	public, private	data integrity, transparency	Permissioned
S4	Healthcare	Hyperledger Fabric	private	Data Integrity, confidentiality, data privacy	permissioned
S5	IOT	Ethereum	public, private	Integrity, confidentiality, architectural security	permissioned
S6	EHR	Ethereum	public	Security, data integrity	permissioned
S7	Multi-cloud application	NA	NA	Authentication, security performance	NA
S8	Cloud application	Ethereum	public	Forensic security analysis, architectural security	permissioned
S9	Cloud-based application	Ethereum	public	NA	Permissionless
S10	Service Orchestration	Ethereum and Hyperledger	public, private	Integrity, confidentiality	permissioned
S11	Multi-cloud system	-	Consortium blockchain	Confidentiality, transparency, integrity	permissioned
S12	API based Application	Ethereum	private, public	Authentication, Data Integrity	permissioned
S13	Oracle	Oracle	private	Integrity, transparency	permissioned
S14	IOT	Ethereum	private, public	Authenticity, integrity, performance	Permissioned
S15	Bifröst application	Ethereum	private	Integrity, semantic security	permissioned
S16	SLA multi-cloud application	NA	NA	Interoperability, fault tolerance and scalability	permissioned
S17	SSI	Hyperledger Fabric	public, private	Integrity, confidentiality	permissioned
S18	Multi-cloud application	Ethereum	public, private	Confidentiality, data integrity	permissioned
S19	Healthcare	-	Consortium blockchain	Confidentiality, integrity, and security features	permissioned
S20	Service orchestration	NA	NA	Confidentiality, security, and compliance	NA
S21	IOT	Local Blockchain	private	Transparency, data integrity	permissioned
S22	Application based on container	Ethereum	private	Integrity, security assets	permissioned
S23	Northbound interface	Hyperledger fabric	private	Authentication, authorization, confidentiality	permissionless
S24	Multi-Cloud Architectures	NA	private	Audit, automation, secure transaction	NA

The S23 and S24 studies focus on SLA security, whereas the rest focus more on blockchain-based security in cloud systems.

Applications that are more potent, scalable, and secure might result from integrating the cloud with other technologies. Blockchain technology is reliable for securing user and resource usage. Still, it cannot completely prevent all six attack vectors in cloud or multi-cloud systems, according to research (e.g., IAM security, APIs, and data storage).

Many studies have examined blockchain-based data security, but there will always be drawbacks or weaknesses when data is exchanged or altered between parties. Reference [11] describes how integrating blockchain technology with IAM and OAuth2.0 for user authentication to access or consume various services might help secure cloud or multi-cloud system services. The main obstacles to system security, though, include ensuring system security when data is exchanged with third parties, identifying architectural flaws, and maintaining the system's service level agreements (SLAs).

5.1. Taxonomy of Blockchain-Based Multi-Cloud Security

One of the newest and fastest-growing technologies is blockchain, and its uses are starting to go beyond banking.

Table 7 highlights the most popular blockchain solutions and platforms, including Ethereum and Hyperledger Fabric, for their many benefits, such as decentralization, immutability, transparency, auditability, and smart contracts.

Although blockchain technology is secure in and of itself, data modification and transmission between third parties can threaten security. We will attempt to address each reported blockchain-based security dimension in the sections that follow.

5.1.1. Architecture

Blockchain technology is secure, but there are still issues with infrastructure, scalability, and energy use. Integrating blockchain with cloud services can reduce these challenges and enhance the development and deployment of secure, decentralized apps. Studies indicate that combining blockchain technology with a hybrid cloud architecture yields dependable and secure systems. Regarding vulnerabilities, the 51% attack is widely recognized as the most prominent weakness in blockchain-based systems.

In the architecture dimension, the main contributions of blockchain are decentralized trust anchors, immutable topology records, and auditability. However, it does not directly detect hidden multi-stage attacks over heterogeneous cloud infrastructures.

The blockchain network's new agreements, protocols, and governance systems make it easier to plan such attacks. Furthermore, the majority of industrial blockchain applications are private blockchains, since they follow protocols and consensus mechanisms that best meet their security, regulatory, and governance constraints, even if doing so means departing from core blockchain concepts. As a result of public blockchains' high processing capacity and the introduction of new consensus algorithms, such as Proof of Stake, which currently dominate the market, the 51% attack has become less common. With private or permissioned blockchains, on the other hand, this is not the case because the transaction validation method is more susceptible to localized intrusions.

Thanks to artificial intelligence and machine learning, issues with performance and vulnerability management in the blockchain-based cloud system are becoming less common. We have found that we can develop safe, high-performance applications by combining proprietary encryption or ciphering between resources with hybrid cloud and hybrid blockchain integration. Businesses can select the location for hosting their tasks based on performance, security, and compliance standards, thanks to the hybrid cloud.

5.1.2. API

A wide variety of cyberattacks may target APIs. To raise awareness of these hazards, the Open Web Application Security Project (OWASP) has compiled a list of API vulnerabilities. Blockchain technology can enhance API security, enabling the safe and effective use of cloud resources. Additionally, blockchain suggests API searchability [50]. Birfröst, an API for Cross-Blockchain interoperability based on notaries, has been suggested. In other words, Cross-Blockchain application developers now have numerous ways to communi-

cate between Cross-Blockchain platforms without having to concern themselves with each Cross-Blockchain platform's implementation or technical specifications.

Blockchain can provide signed transactions, decentralized verification, and tamper-proof API audit trails to secure APIs. However, it remains insufficient for detecting abnormal API call sequences without AI-based correlation. To use blockchain technology to secure an API system, implement a blockchain-based API authentication and authorization system, set up a regular blockchain-based auditing system, and monitor for unusual activity. Blockchain-based security must be combined with additional security measures or best practices to guarantee the security of an API-based system. An analysis of the Oracle blockchain concluded that it comprises off-chain components (such as data providers) that connect the blockchain to the outside world and smart contracts implemented as application programming interfaces (APIs).

5.1.3. Authentication

Blockchain technology is essential to authentication security, especially for identity and access control. Identity and access management (IAM) is crucial for organizations because it enables them to identify, authenticate, and authorize users of services or systems. Most research on blockchain and cloud computing has focused on IAM and storage. As it stands, using blockchain-based identity management systems to access or use cloud resources is an effective way to enhance authentication and authorization in cloud environments while reducing risk for CSPs.

Blockchain-based identity management and verifiable credentials improve identity traceability and reduce reliance on centralized identity providers for authentication and IAM. Nameless, statistical, and machine-learning-based detection is still needed to identify behavioral identity anomalies and privilege abuse.

Using OAuth 2.0 in conjunction with blockchain-based IAM provides a more adaptable and secure way to control access to cloud resources. The proposed approach uses blockchain technology for authorization and authentication to build a secure, decentralized identity and access management system. The OAuth 2.0 approach ensures secure, granular access control to sensitive data stored on the Fabric network and Hyperledger Fabric. Numerous prior studies across a variety of industries have abundantly demonstrated the usefulness of blockchain in IAM security. According to experiments, the safest and most efficient IAM systems are those that use dual identification or integrate it with other identity modalities or security models.

By allowing users to maintain independent identities on the blockchain, identity theft is less likely to occur. Blockchain-based identity management helps many industries by reducing GDPR-related fines and data breaches. Self-sovereign identification (SSI), when combined with artificial intelligence and blockchain, can be a key component of facial recognition technology.

5.1.4. Multi-Cloud Automation and Orchestration

An increasing number of businesses are using automation and orchestration to enhance their systems in light of the advent of cloud computing. In any event, neither customers nor organizations stand to gain from incorporating blockchain technology across the full automation process. However, to protect and optimize the automation system, we can incorporate this technology into certain parts of the procedure (such as authentication). This section examines organizational security in multi-cloud automation and discusses the security of cloud automation. It lists the many layers of the infrastructure that could be attacked during the automation process. Indeed, blockchain can be useful for data

storage throughout the orchestration process and for providing authentication for various automation and orchestration resources, thereby reducing security risks during automation.

5.1.5. SLA Management (Security Accountability Domain)

SLA violations are not attack vectors in the traditional sense, but they are measurable risk amplifiers and indirect indicators of an attack (e.g., induced downtime that masks lateral movement). As such, they are included in the security dimension taxonomy. This contrasts with the previous technical threat surfaces.

To maintain a specific quality of service (quality of service) and keep performance above a certain level, cloud service providers (CSPs) and customers must agree on Service Level Agreements (SLAs). Blockchain offers new options for addressing the challenges of automated SLA monitoring and administration. While integrating blockchain into SLAs between CSPs is challenging, if we want a safe and effective system, blockchain can aid in SLA-level audits, vulnerability identification, and intrusion warnings. To establish a trusting environment for users, ref. [52] suggests a system built on the Hyperledger Fabric blockchain to verify or detect SLA-level violations.

5.1.6. Cybersecurity Compliance (Governance and Auditability Domain)

While not a direct route to assault, cybersecurity compliance is a governance and auditability domain. However, this dimension is operationally significant to the SOC-LLM Explanation Agent's evidence-to-compliance mapping function, as compliance deficiencies expose businesses to untested configurations and inadequate audit trails that attackers might exploit.

Cybersecurity legislation does not fully acknowledge the significance of blockchain. Blockchain technology by itself is insufficient to guarantee the security of these systems and to create a dependable, efficient, and safe system. Blockchain technology is safe in and of itself, but security guidelines and regulations must be followed to keep the system secure, especially when users must exchange data with other parties.

Security problems across multiple providers are common in multi-cloud environments. Blockchain provides a single layer of security. As blockchain technology advances, artificial intelligence and machine learning will enable us to build effective multi-cloud systems.

The reviewed studies show that blockchain contributes differently across security dimensions. For this reason, a taxonomy based on security dimensions is more useful than a generic blockchain–cloud taxonomy. Table 8 summarizes the main mapping. The distribution of the examined corpus across the six attack-vector dimensions is shown in Figure 3. As shown, there are five studies on architecture and API security, three on IAM/authentication and orchestration, one on SLA management, and seven on cross-cutting security issues spanning multiple dimensions

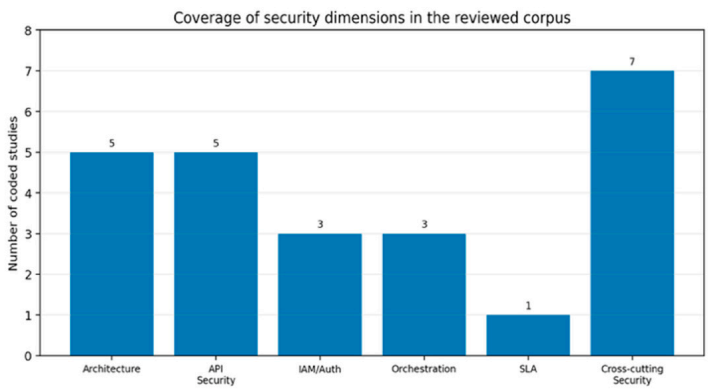

Figure 3. Coverage of attack-vector dimensions in the reviewed corpus.

Table 8. Taxonomy of security dimensions in blockchain-enabled multi-cloud systems, distinguishing technical attack surfaces from governance and accountability domains.

Security Dimensions	Typical Risk in Multi-Cloud Systems	Blockchain Contribution	Remaining Gap Addressed by SOC-LLM
Architecture	Fragmented trust boundaries, workload placement risk, lack of unified audit	Immutable topology evidence, trusted service registry, decentralized trust anchors	Detect hidden multi-stage patterns and reason over cross-cloud context
API (Application Programming Interface) security	Token abuse, weak authorization, excessive privileges, API (Application Programming Interface) call manipulation	Signed API (Application Programming Interface) transactions, smart-contract audit trails, decentralized API (Application Programming Interface) verification	Correlate API (Application Programming Interface) sequences, explain suspicious behavior and recommend containment
IAM (Identity and Access Management)/authentication	Credential compromise, role abuse, federation weaknesses, identity theft	Decentralized identity, verifiable credentials, auditable access decisions	Identify anomalous identity behavior and explain why access is suspicious
Orchestration and automation	Compromised CI/CD (Continuous Integration and Continuous Delivery/Deployment), malicious infrastructure-as-code, container drift	Trusted workflow records, policy enforcement, tamper-resistant deployment logs	Detect orchestration drift and investigate tool-chain anomalies
SLA (Service Level Agreement) management	Unverifiable downtime, performance disputes, responsibility ambiguity	Smart contracts for SLA (Service Level Agreement) evidence and violation records	Predict SLA (Service Level Agreement) degradation and correlate it with incidents
Cybersecurity compliance	Fragmented evidence, privacy risks, incomplete auditability	Immutable evidence chain, access traceability, accountability	Mapping technical evidence to compliance requirements and generate audit-ready explanations

5.2. Blockchain-Based Security Solutions and Comparative Analysis of Reviewed Studies

The reviewed studies show that blockchain primarily supports trust establishment, decentralized identity management, immutable auditability, smart-contract-based policy enforcement, and tamper-resistant evidence management. These capabilities are particularly useful for authentication, API traceability, SLA verification, and compliance auditing. However, blockchain-based mechanisms remain limited in defending against intelligent, distributed, and evolving attacks, as they mainly record and validate events rather than interpret their security implications.

Table 9 compares the major security approaches identified in this review. Blockchain-only solutions offer strong traceability and integrity but limited capabilities for proactive detection and explanation. SIEM-based solutions improve event correlation but are often constrained by rule dependency and alert fatigue. ML-based approaches improve anomaly detection but may lack explainability and forensic traceability. LLM-based approaches can improve reasoning and contextual explanations but require governance mechanisms to reduce hallucinations and ensure reliability. In contrast, SOC-LLM-enhanced security combines blockchain evidence management, statistical anomaly detection, machine learning, SIEM/SOAR workflows, and multi-agent LLM reasoning. This combination provides a more complete security model that includes detection, explanation, traceability, and response support.

These results motivate deploying a SOC-LLM-augmented architecture that uses blockchain as a trust and evidence layer, statistical analysis, machine learning, and multi-agent LLM reasoning to enable proactive detection, contextual explanation, and response support. Section 2.4 elaborates on the SOC-LLM framework's positioning relative to security copilot systems (e.g., Microsoft Security Copilot) and agent-based architectures (e.g., PentestGPT, Auto-Defense); the key differentiators are blockchain-grounded evidence integrity and the hierarchical supervisory agent mechanism.

Table 9. Comparative security capabilities of alternative approaches.

Approach	Detection	Explanation	Evidence Integrity	Response Support	Main Limitation
Blockchain only	Low to medium	Low	High	Low	Records events but does not interpret attack intent
SIEM/rules only	Medium	Medium	Medium	Medium	High false positives and limited cross-cloud reasoning
ML anomaly detection only	Medium to high	Low	Low to medium	Low	Black-box decisions and weak forensic evidence
LLM only	Medium	High	Low	Medium	Hallucination and lack of trusted evidence
SOC-LLM + ML + blockchain	High potential	High	High	High	Requires governance, validation and benchmarking

6. Proposed SOC-LLM-Augmented Architecture

Blockchain should be integrated into a more comprehensive SOC-LLM architecture. The tiers of this architecture perform trust, detection, reasoning, human validation, and response functions. Blockchain technology can provide decentralized, tamper-proof, and immutable evidence. Statistical detectors based on machine learning (ML) produce numerical anomaly scores. LLM agents handle investigation, correlation, and explanation. SOAR workflows execute controlled response actions, while human analysts verify the final determination. The analysis shows that blockchain alone cannot secure the multi-cloud system. This solution has been added to improve the security of these systems further. Figure 4 shows the proposed SOC-LLM architecture for this analysis. A preliminary simulation-based validation strategy for this architecture, including evaluation metrics and baseline comparisons, is outlined in Section 6.8.

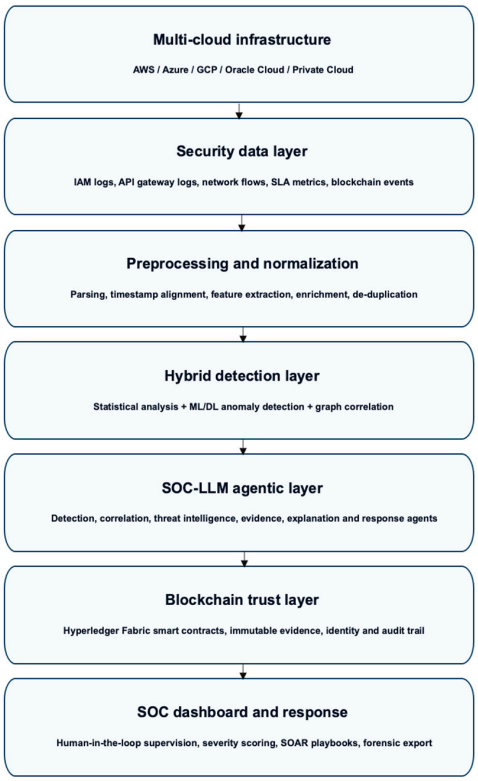

Figure 4. The proposed SOC-LLM- Augmented Architecture.

6.1. Security Data Layer

The data layer collects information from a variety of sources, including logs, metrics, and events from internal systems and cloud service providers. Examples of input data

include IAM events, API gateway requests, management plane audit logs, Kubernetes events, container runtime alerts, network flows, DNS activity, cloud storage access logs, SLA metrics, and blockchain transaction logs. Each event is standardized with a dataset that includes time, origin, user, source, identity, asset, action, outcome, risk score, and proof hash. When integrity is critical, the proof hash is stored on the blockchain. This supports our monitoring, analysis, and decision-making.

Our blockchain-based SOC-LLM architecture addresses the security of diverse data sources, including multimedia streams, medical images, surveillance video feeds, and AI-generated content, as well as conventional log audits and transaction integrity verification.

Consequently, using multimedia integrity verification modules alongside traditional blockchain auditing techniques could be advantageous for future SOC-LLM systems. This development will enhance end-to-end security assurance in next-generation cloud ecosystems by enabling security operations centers to extend trust from text-based logs and transactions to complex multimedia evidence.

6.2. Statistical and Machine-Learning Detection Layer

This first layer of analysis involves preprocessing and normalization and combines statistical analysis with machine learning (ML). Statistical Detectors: z-score thresholds, weighted exponential moving averages, entropy analysis, frequency deviation, time-window correlation, and seasonality-aware backcross marks. Machine learning (ML) and deep learning (DL) models include techniques such as isolation forests, single-class SVMs, random forests, autoencoders, LSTM/Transformer architectures, and graph-based anomaly detection. This hybrid approach eliminates the need for a single sensor and enables the SOC to detect both simple deviations and complex anomalies across multiple sources [53].

6.3. SOC-LLM Agentic Layer

Specialized agents make up the SOC-LLM layer. The detection agent identifies suspicious trends by aggregating unfiltered notifications, while the correlation agent searches across vendors for similar events. The RAG threat intelligence agent draws on the incident log, vulnerability documentation, MITRE-like databases, and internal response playbooks for contextual information. The blockchain verification agent compares logs and evidence hashes with the registry. The explanatory agent generates a summary report for analysts. The reaction planner recommends containment measures and anticipated outcomes. A supervisor checks for consistency, identifies misinformation, and demands conclusions supported by facts. Each agent has a specific role in the system. Table 10 outlines the main role, inputs, and outputs for each agent in the proposed SOC-LLM layer.

Table 10. Specialized agents in the proposed SOC-LLM layer.

Agent	Main Role	Input	Output
Detection agent	Classify and prioritize suspicious events	Alerts, anomaly scores, SIEM events	Initial incident hypothesis
Correlation agent	Link events across clouds and time windows	Logs, identities, assets, network flows	Attack timeline and related evidence
RAG threat-intelligence agent	Retrieve grounded context	Incident hypothesis and indicators	Relevant tactics, vulnerabilities and playbooks
Blockchain evidence agent	Verify evidence integrity	Log hash, transaction ID, smart contract state	Evidence validation report
Explanation agent	Generate analyst-readable reasoning	Correlated events and verified evidence	Incident explanation and confidence
Response planner	Recommend containment and recovery actions	Incident severity and business context	SOAR-ready response plan
Oversight agent	Control hallucination and contradiction	All agent outputs	Approved, rejected or revised investigation

Each agent has a unique role description or task specialization that clearly defines a cybersecurity duty, operational boundaries, expected outputs, and required inputs. The security context, which includes threat intelligence, blockchain transaction trails, cloud infrastructure logs, prior alerts, and agent choices, binds agents. LLM-generated decisions are guaranteed to follow SOC procedures thanks to validation requirements and output formatting restrictions. For example, the Explanation Agent is restricted to producing human-interpretable reasoning based only on existing security evidence. Meanwhile, the Oversight Agent's prompt now states its function as a supervisory element that reviews the coherence of results from other agents.

6.4. Blockchain Trust Layer

According to our analysis, the blockchain trust layer should be built on a tried-and-true platform such as Hyperledger Fabric to succeed in this sector, particularly if the desired environment is a multi-cloud system for businesses. Hyperledger Fabric supports membership services, private channels, chaincode, endorsement policies, and access governance. It is also adaptable and can be tailored to meet specific needs. The blockchain layer of the suggested architecture stores hashes of crucial logs, event proofs, smart contract resolutions, SLA non-compliance records, and response verifications. Sensitive information is kept outside the process to preserve secrecy and minimize the size of the blockchain.

6.5. SOC Dashboard and Response

A SOC-LLM system must, however, always include human intervention. The dashboard must display real-time warnings, severity indicators, attack progression, evidence verification, deployed resources, confidence levels, recommended response measures, and analyst suggestions. Instead of using unverifiable language, every conclusion produced by the LLM must reference evidence identifiers. Except for pre-established low-risk containment measures, the interface should allow analysts to accept, reject, or modify the response plan before execution.

6.6. Agent Collaboration Workflow and Prompt-Constrained Reasoning

While the specialized agents that comprise the SOC-LLM layer are listed in Table 10, an important aspect of the implementation concerns how these agents work together to detect uncontrolled LLM reasoning; as a result, the architecture shown here provides a hierarchical, evidence-based workflow in which each agent produces structured output rather than free-form natural language and operates within predetermined contextual limitations. This multi-agent cooperation process is depicted in Figure 5, which shows the message flow from initial event detection through blockchain evidence verification, correlation, explanation, and supervisory confirmation prior to findings being displayed on the SOC dashboard.

The procedure begins when blockchain monitoring systems, cloud services, identity management platforms, authentication services, or statistical anomaly detectors generate security events. These events are first normalized to a common model and then forwarded to the detection agent. The detection agent performs an initial analysis using anomaly indicators derived from statistical methods, machine-learning classifiers, and security rules. The agent does not conclude; instead, it formulates attack hypotheses with confidence scores and identifiers to support the evidence.

The blockchain evidence agent, meanwhile, validates the integrity of the collected evidence using blockchain records. More specifically, it verifies transaction IDs, log hashes, smart contract states, and any audit trails present in the blockchain infrastructure. Afterward, the evidence can be considered valid for further investigation.

Once the evidence is verified, the correlation and explanation functions aggregate events across cloud environments and transform machine-readable detections into justifications for analysts. All explanations remain strictly linked to the verified evidence references and confidence scores. The response planner receives the corresponding incident report, along with business context, severity assessment, and operational constraints. It then generates candidate containment and recovery actions that comply with the organization's policies.

Finally, the supervisory agent verifies the outcomes produced by every preceding agency. Before approving publication on the SOC dashboard, it conducts consistency checks, identifies inconsistencies, detects "hallucinations," and confirms policy compliance.

In this hierarchical cooperation architecture, no LLM agent may issue security judgments unilaterally without first completing the steps of evidence evaluation and supervisor verification.

```
+--------+     +---------+     +-------+     +---------+     +-------------+
|  User  |     | ArcFace |     | FAISS |     | Fabric  |     | Detection   |
+--------+     +---------+     +-------+     +---------+     +-------------+
    |               |              |              |                |
    | Auth Request  |              |              |                |
    |-------------->|              |              |                |
    |               | Extract Emb. |              |                |
    |               |------------->|              |                |
    |               |              | Similarity   |                |
    |               |              |------------->|                |
    |               |              |              | Verify User    |
    |               |              |              |--------------->|
    |               |              |              |                |
    |               |              |              | Security Event |
    |               |              |              |--------------->|
    |               |              |              |                |
    |               |              |              |                v
    |               |              |              |      Correlation Agent
    |               |              |              |                |
    |               |              |              |                v
    |               |              |              |      Explanation Agent
    |               |              |              |                |
    |               |              |              |                v
    |               |              |              |      Oversight Agent
    |               |              |              |                |
    |               |              |              |                v
    |               |              |              |      SOC Dashboard
```

Figure 5. Multi-Agent Collaboration Process in the Proposed SOC-LLM Architecture.

6.7. Prompt Templates and Contextual Constraints

To improve repeatability, each LLM-based agent uses a preset query template and accepts only structured cybersecurity evidence. This architecture minimizes the risk of hallucinations while ensuring deterministic behavior.

The integration of SOC-LLM offers an important audit prompt for our system, which is built on blockchain-based facial recognition technology, for example:

- For Oversight Agent Prompt:

System Role:
You are the Oversight Agent for a Security Operations Center.
Mission:
Validate attack assessments produced by subordinate agents.
Constraints:
• Use only the supplied evidence.
• Do not introduce external facts.
• Reject conclusions not supported by evidence.
• Output must follow the specified JSON schema.
Input:
{
"incident_id": "INC-245",
"attack_type": "Authentication Abuse",
"confidence": 0.91,
"severity": "HIGH",
"evidence_ids": ["TX1045","LOG782","AUTH558"]
}
Output:
{
"validated": true,
"risk_score": 92,
"recommended_action": "Temporarily block the account and initiate identity verification."
}

- For Explanation Agent Prompt:

System Role:
You are an Explanation Agent supporting SOC analysts.
Mission:
Transform technical detections into human-readable incident reports.
Constraints:
• Explain only verified evidence.
• Do not generate new facts.
• Maintain traceability to evidence identifiers.
Input:
{
"attack_type": "Credential Abuse",
"severity": "HIGH",
"confidence": 0.94,
"evidence": ["AUTH558","TX1045","LOG782"]
}
Output:
A concise, analyst-oriented explanation of the attack rationale, supporting evidence, potential impact, and recommended investigative actions.

6.8. Preliminary Validation Strategy and Simulation Protocol

To provide a preliminary empirical foundation for assessing the feasibility of the proposed SOC-LLM architecture, we present a simulation-based validation method that

uses multi-cloud and blockchain logs and is built on a face recognition system integrating Arc-Face and FAISS. However, the specifics of the implementation are not provided in this article, even though a few sample instances were mentioned above. This method is intended to be replicable using a private system, open-source tools, and public reference datasets, enabling future studies to replicate it independently. Three representative attack scenarios are selected to evaluate the end-to-end agent pipeline: (i) a credential abuse scenario targeting the IAM layer; (ii) a malicious API call chain scenario; and (iii) an SLA degradation incident correlated with an orchestration anomaly. For each scenario, detection rate, false positive rate, mean time to explain, evidence validation accuracy, and agent response agreement rate are reported. A SIEM-rules-only baseline and an ML-anomaly-only baseline are used for comparison under the same synthetic log corpus. The agents' proposals, following this simulated attack on our blockchain-based facial recognition system, are shown above.

7. Limits and Future Directions

Although the systematic methodology used in this literature review analysis reduces selection bias, the following limitations should be noted.

The literature analysis identifies several research gaps:

- Blockchain-enabled multi-cloud systems lack standardized security mechanisms.
- Scalability constraints of blockchain consensus mechanisms.
- Limited interoperability among cloud service providers.
- Inadequate criteria for evaluating cloud security solutions based on blockchain technology.

For proactive threat identification and security monitoring, future research should focus on hybrid architectures that integrate blockchain technology with artificial intelligence. Subsequent research could focus on several areas. First, to ensure resource security in multi-cloud systems, use blockchain, AI, and machine learning to conduct real-time audits, thereby providing a safe and effective system. Second, use AI and blockchain for authentication and authorization in multi-cloud systems, leveraging facial recognition or other biometric methods.

This may be achieved by providing them with access to a seamless, secure authentication method that works across various domains. Thirdly, to reduce vulnerabilities, integrate blockchain technology into cloud automation and orchestration operations. To further enhance system security and dependability, incorporate machine learning algorithms and quantum computing to ensure security and detect anomalies and potential attacks.

The following summary demonstrates the blockchain's potential to enhance decentralized trust, integrity, and traceability. However, these characteristics do not always identify an attack. A hacked administrator can still complete valid transactions. A malicious API sequence can remain unchanged on the ledger. A smart contract can detect an SLA breach but cannot explain why. Therefore, blockchain must be used in conjunction with statistical surveillance, behavioral analysis, and human-guided reasoning to provide a proactive defense.

The literature considered AI a potential future direction, but rarely discussed how to implement it within the SOC. The proposed architecture addresses this gap by clearly assigning responsibilities to statistical detectors, automated learning models, LLM agents, intelligent blockchain contracts, and human analysts. The SOC-LLM layer does not replace the blockchain layer; rather, it converts the blockchain's problems into exploitable investigation paths. It explains, correlates, and contextualizes machine learning outcomes rather than replacing them. Table 11 presents the evaluation, the main challenges, and mitigation strategies for SOC-LLM deployment.

Table 11. Main challenges and mitigation strategies for SOC-LLM deployment.

Challenge	Risk	Mitigation Strategy
LLM hallucination	Incorrect explanations or unsupported recommendations	Evidence-grounded RAG, oversight agent, citation of log IDs, human validation
Data privacy	Sensitive logs exposed to LLM or third-party services	Local/private LLMs, redaction, access controls, on-chain hashes only
Real-time scalability	High latency from multi-agent reasoning and blockchain writes	Fast/slow pipeline, model distillation, selective on-chain anchoring, batching
Dataset scarcity	Limited labeled multi-cloud attack data	Synthetic log generation, cyber range simulation, weak supervision, transfer learning
Interoperability	Different cloud logs, IAM models and APIs	Common event schema, adapters, Open Telemetry-like normalization
Explainability	Black-box ML and complex agent traces	Structured incident narratives, feature attribution, timeline visualization
Governance	Uncontrolled automation may cause business disruption	Approval workflows, risk-based automation, rollback procedures

This systematic analysis has allowed us to highlight recent advances and current limitations in blockchain-based security for multi-cloud systems, with a focus on attack vectors. It has also helped establish a solid, well-organized foundation for clearly identifying the areas that should be prioritized for further scientific research.

Additionally, this enabled us to propose a SOC-LLM-augmented architecture to enhance proactive, explainable, and auditable attack detection in blockchain-enabled multi-cloud systems. The proposed framework combines blockchain-based evidence integrity, statistical and ML-based anomaly detection, LLM-driven contextual reasoning, and SOC/SOAR response workflows, unlike blockchain-only, SIEM-only, ML-only, or LLM-only approaches.

A preliminary simulation-based validation strategy is outlined in Section 6.8, covering three representative attack scenarios, five evaluation metrics, and a comparison with SIEM-only and ML-only baselines. Full empirical validation through operational deployment in a live multi-cloud testbed remains a priority for future work.

8. Conclusions

In conclusion, we conducted a systematic literature review to evaluate the security of multi-cloud blockchain systems. We considered six previously recognized attack points or attack vectors: architecture, authentication, automation, SLAs, and cybersecurity laws. Using a PRISMA-based approach, we analyzed 24 peer-reviewed studies on the security features of multi-cloud blockchain systems. The findings demonstrate that while blockchain alone cannot secure a multi-cloud system (i.e., apps built across different clouds), combining it with other security techniques can provide a strong, secure system.

Blockchain has clearly demonstrated its benefits in authentication and storage security across these six attack vectors, and it improves transparency, authentication, and data integrity in distributed cloud environments.

However, given rapid technological advances and the lack of standardized frameworks for multi-cloud environments, future research should focus on developing scalable blockchain infrastructures, integrating artificial intelligence for automated security monitoring, and creating interoperable frameworks to secure complex multi-cloud environments. This work proposes a SOC-LLM layer to address gaps in proactive detection and explainability identified in the reviewed literature. Architecturally, integrating SOC-LLM capabilities with blockchain has the potential to shift multi-cloud security from passive auditability to proactive, explainable, and human-in-the-loop cyber defense. These conclusions reflect a design intent grounded in the systematic analysis of the reviewed literature.

Empirical validation of the proposed framework, using simulations conducted on our system, required an evaluation of the architecture's effectiveness; however, the details and discussion of this implementation are beyond the scope of this review.

Author Contributions: Conceptualization, A.K.A.A.; methodology, A.K.A.A.; software, A.K.A.A.; validation, A.K.A.A., and H.C.; formal analysis, A.K.A.A.; investigation, A.K.A.A.; resources, A.K.A.A. and H.C.; data curation, A.K.A.A.; writing—original draft preparation, A.K.A.A.; writing—review and editing, A.K.A.A. and H.C.; visualization, A.K.A.A. and H.C.; supervision, A.K.A.A. and H.C.; project administration, H.C. and A.K.A.A.; funding acquisition, A.K.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All the relevant data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Columbus, C. Ensuring Secure and Efficient Multi-Cloud Storage with Brotli Compression and Hierarchical Data Protection. *Res. Sq.* **2023**. [CrossRef] [PubMed]
2. Khanna, A.; Sah, A.; Bolshev, V.; Burgio, A.; Panchenko, V.; Jasiński, M. Blockchain–Cloud Integration: A Survey. *Sensors* **2022**, *22*, 5238. [CrossRef] [PubMed]
3. Kumar, M.; Maple, C.; Chand, S. An Efficient and Secure Identity-Based Integrity Auditing Scheme for Sensitive Data with Anti-Replacement Attack on Multi-Cloud Storage. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101745. [CrossRef]
4. Miyachi, K.; Mackey, T.K. hOCBS: A Privacy-Preserving Blockchain Framework for Healthcare Data Leveraging an on-Chain and off-Chain System Design. *Inf. Process. Manag.* **2021**, *58*, 102535. [CrossRef]
5. Yu, H.; Hu, Q.; Yang, Z.; Liu, H. Efficient Continuous Big Data Integrity Checking for Decentralized Storage. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1658–1673. [CrossRef]
6. Rosini, A.; Mestriner, D.; Labella, A.; Bonfiglio, A.; Procopio, R. A Decentralized Approach for Frequency and Voltage Regulation in Islanded PV-Storage Microgrids. *Electr. Power Syst. Res.* **2021**, *193*, 106974. [CrossRef]
7. Mishra, R.; Ramesh, D.; Edla, D.R.; Qi, L. DS-Chain: A Secure and Auditable Multi-Cloud Assisted EHR Storage Model on Efficient Deletable Blockchain. *J. Ind. Inf. Integr.* **2022**, *26*, 100315. [CrossRef]
8. Li, D.; Du, R.; Au, M.H.; Fu, Y. Meta-Key: A Secure Data-Sharing Protocol under Blockchain-Based Decentralised Storage Architecture. *IEEE Netw. Lett.* **2019**, *1*, 30–33. [CrossRef]
9. Demertzis, K.; Rantos, K.; Magafas, L.; Skianis, C.; Iliadis, L. A Secure and Privacy-Preserving Blockchain-Based XAI-Justice System. *Information* **2023**, *14*, 477. [CrossRef]
10. Enge, A.; Satybaldy, A.; Nowostawski, M. An Offline Mobile Access Control System Based on Self-Sovereign Identity Standards. *Comput. Netw.* **2022**, *219*, 109434. [CrossRef]
11. Sutradhar, S.; Karforma, S.; Bose, R.; Roy, S.; Djebali, S.; Bhattacharyya, D. Enhancing Identity and Access Management Using Hyperledger Fabric and OAuth 2.0: A Block-Chain-Based Approach for Security and Scalability for Healthcare Industry. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 49–67. [CrossRef]
12. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A Systematic Literature Review of Blockchain Cyber Security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
13. Sudarsan, S.V.; Schelen, O.; Bodin, U. Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT. *IEEE Access* **2021**, *9*, 98169–98184. [CrossRef]
14. Sim, W.L.; Chua, H.N.; Tahir, M. Blockchain for Identity Management: The Implications to Personal Data Protection. In *Proceedings of the 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 19–21 November 2019*; IEEE: Piscataway, NJ, USA, 2019; pp. 30–35.
15. Ferrag, M.A.; Ndhlovu, M.; Tihanyi, N.; Cordeiro, L.C.; Debbah, M.; Lestable, T.; Thandi, N.S. Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices. *IEEE Access* **2023**, *12*, 40. [CrossRef]
16. Deng, G.; Liu, Y.; Mayoral-Vilches, V.; Liu, P.; Li, Y.; Xu, Y.; Zhang, T.; Liu, Y.; Pinzger, M.; Rass, S. PentestGPT: An LLM-Empowered Automatic Penetration Testing Tool. *arXiv* **2023**, arXiv:2308.06782.
17. Xu, J.; Stokes, J.W.; McDonald, G.; Bai, X.; Marshall, D.; Wang, S.; Swaminathan, A.; Li, Z. AutoAttacker: A Large Language Model Guided System to Implement Automatic Cyber-Attacks. *arXiv* **2024**, arXiv:2403.01038.

18. Zeng, C.; He, D.; Feng, Q.; Yang, X.; Luo, Q. SecureGPT: A Framework for Multi-Party Privacy-Preserving Transformer Inference in GPT. *IEEE Trans. Inform. Forensic Secur.* **2024**, *19*, 9480–9493. [CrossRef]
19. Reece, M.; Lander, T.E., Jr.; Stoffolano, M.; Sampson, A.; Dykstra, J.; Mittal, S.; Rastogi, N. Systemic Risk and Vulnerability Analysis of Multi-Cloud Environments. *arXiv* **2023**, arXiv:2306.01862.
20. Checkpoint Software. *Cloud Security Report: Check Point Software*; Checkpoint Software: Tel Aviv, Israel, 2022.
21. Zhang, Y.; Geng, H.; Su, L.; Lu, L. A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage. *IEEE Access* **2022**, *10*, 105920–105929. [CrossRef]
22. Zahed Benisi, N.; Aminian, M.; Javadi, B. Blockchain-Based Decentralized Storage Networks: A Survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656. [CrossRef]
23. Sabeena, S.J.; Vijila, S.A. Blockchain-Based Solution for Securing Job Card Data Integrity and Payment System Using Bi-Quad Merkle Tree. *Int. J. Intell. Syst. Appl. Eng.* **2024**, *12*, 314–328.
24. Gujar, V. Identity management, SSI and blockchain: A review. *Int. J. Sci. Res.* **2023**, *8*, 38–45. [CrossRef]
25. Alamri, B.; Crowley, K.; Richardson, I. Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review. *IEEE Access* **2022**, *10*, 59612–59629. [CrossRef]
26. Vakilinia, I.; Wang, W.; Xin, J. An Incentive-Compatible Mechanism for Decentralized Storage Network. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 2294–2306. [CrossRef]
27. Aldriwish, K. A Double-Blockchain Architecture for Secure Storage and Transaction on the Internet of Things Networks. *Int. J. Comput. Sci. Netw. Secur.* **2021**, *21*, 119–126. [CrossRef]
28. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Keele University: Keele, UK, 2004.
29. Gangadhara, B. Exploiting AI and source blockchain framework to mitigate risks in cloud manufacturing in industry 3.0. *Int. J. Multidiscip. Eng. Curr. Res.* **2021**, *6*, 11–26.
30. Zahir, A.; Groshev, M.; Antevski, K.; J.Bernardos, C.; Ayimba, C.; De La Oliva, A. Performance Evaluation of Private and Public Blockchains for Multi-Cloud Service Federation. In *Proceedings of the 25th International Conference on Distributed Computing and Networking, Chennai, India, 4 January 2024*; ACM: New York, NY, USA, 2024; pp. 217–221.
31. SH, A.S.; TS, L.P.; Sunitha, T.; Sriman, B.; NK, S.K.; Subin, S.S. A Secure and Efficient Blockchain-Based Multi-Cloud Medical File Sharing. In *Proceedings of the 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*; IEEE: Piscataway, NJ, USA, 2023; pp. 1–7.
32. Irshad, R.R.; Hussain, S.; Hussain, I.; Nasir, J.A.; Zeb, A.; Alalayah, K.M.; Alattab, A.A.; Yousif, A.; Alwayle, I.M. IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain Based Approach Towards a Trustworthy Cloud Computing. *IEEE Access* **2023**, *11*, 105479–105498. [CrossRef]
33. Sravanthi, K.; Sekhar, P.C. An Efficient Integrity Verification Based Multi-User Cloud Access Control Framework Using Block Chain Technology on EHR Database. *Int. J. Intell. Syst. Appl. Eng.* **2024**, *12*, 536–549. [CrossRef]
34. Zhou, M.; Xiao, P.; Wang, Q.; Ruan, S.; Chen, X.; Yang, M. Enhancing the Trustworthiness of 6G Based on Trusted Multi-Cloud Infrastructure: A Practice of Cryptography Approach. *CMES-Comput. Model. Eng. Sci.* **2024**, *138*, 957. [CrossRef]
35. Ragu, G.; Ramamoorthy, S. A Blockchain-Based Cloud Forensics Architecture for Privacy Leakage Prediction with Cloud. *Healthc. Anal.* **2023**, *4*, 100220. [CrossRef]
36. Arias Maestro, A.; Sanjuán Martínez, Ó.; Teredesai, A.M.; García-Díaz, V. Blockchain Based Cloud Management Architecture for Maximum Availability. *Int. J. Interact. Multimed. Artif. Intell.* **2023**, *8*, 88–94. [CrossRef]
37. Zeydan, E.; Baranda, J.; Mangues-Bafalluy, J. Post-Quantum Blockchain-Based Secure Service Orchestration in Multi-Cloud Networks. *IEEE Access* **2022**, *10*, 129520–129530. [CrossRef]
38. Wu, Q.; Lai, T.; Zhang, L.; Mu, Y.; Rezaeibagha, F. Blockchain-Enabled Multi-Authorization and Multi-Cloud Attribute-Based Keyword Search over Encrypted Data in the Cloud. *J. Syst. Archit.* **2022**, *129*, 102569. [CrossRef]
39. Ramadhan, A.N.; Pane, K.N.; Wardhana, K.R. Blockchain and API Development to Improve Relational Database Integrity and System Interoperability. *Procedia Comput. Sci.* **2023**, *216*, 151–160. [CrossRef]
40. Pasdar, A.; Lee, Y.C.; Dong, Z. Connect API with Blockchain: A Survey on Blockchain Oracle Implementation. *ACM Comput. Surv.* **2023**, *55*, 1–39. [CrossRef]
41. Baucas, M.J.; Spachos, P. Permissioned Blockchain Reinforced API Platform for Data Management in IoT-Based Sensor Networks. In *Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM)*; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
42. Scheid, E.J.; Kiechl, P.; Franco, M.; Rodrigues, B.; Killer, C.; Stiller, B. Security and Standardization of a Notary-Based Blockchain Interoperability API. In *Proceedings of the 2021 Third International Conference on Blockchain Computing and Applications (BCCA)*; IEEE: Piscataway, NJ, USA, 2021; pp. 42–48.
43. Sivagami, V.M.; EaswaraKumar, K.S.; Jayanthi, D.; Kalavathi, S. Blockchain-Integrated Decentralized Fault Tolerance for Secure and Energy-Efficient Multi-Cloud Interoperability. *Sustain. Comput. Inform. Syst.* **2025**, *47*, 101170. [CrossRef]
44. Zeydan, E.; Baranda, J.; Mangues-Bafalluy, J.; Arslan, S.S.; Turk, Y. A Trustworthy Framework for Multi-Cloud Service Management: Self-Sovereign Identity Integration. *IEEE Trans. Netw. Sci. Eng.* **2024**, *11*, 3135–3147. [CrossRef]

45. Awadallah, R.; Samsudin, A.; Teh, J.S.; Almazrooie, M. An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain. *IEEE Access* **2021**, *9*, 69513–69526. [CrossRef]
46. Son, S.; Lee, J.; Kim, M.; Yu, S.; Das, A.K.; Park, Y. Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain. *IEEE Access* **2020**, *8*, 192177–192191. [CrossRef]
47. Rompicharla, R. Continuous Compliance Model for Hybrid Multi-Cloud through Self-Service Orchestrator. In *Proceedings of the 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*; IEEE: Piscataway, NJ, USA, 2020; pp. 589–593.
48. Verma, R.; Dhanda, N.; Nagar, V. Towards a Secured IoT Communication: A Blockchain Implementation Through APIs. In *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*; Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M., Eds.; Lecture Notes in Networks and Systems; Springer Nature: Singapore, 2023; Volume 421, pp. 681–692.
49. Sun, J.; Wu, C.; Ye, J. Blockchain-Based Automated Container Cloud Security Enhancement System. In *Proceedings of the 2020 IEEE International Conference on Smart Cloud (SmartCloud)*; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
50. Hoang, H.D.; Duy, P.T.; Pham, V.-H. A Security-Enhanced Monitoring System for Northbound Interface in SDN Using Blockchain. In *Proceedings of the Tenth International Symposium on Information and Communication Technology—SoICT 2019, Hanoi, Ha Long Bay, Vietnam, 4–6 December 2019*; ACM Press: New York, NY, USA, 2019; pp. 197–204.
51. Patil, B. Integration of Blockchain with AWS and Azure for Enhanced Cloud Security and Compliance in Multi-Cloud Architectures. In *Proceedings of the 2025 International Conference on Computing and Communication Technologies (ICCCT), Chennai, India, 16 April 2025*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–5.
52. Abhishek, P.M.; Chobari, A.; Narayan, D.G. SLA Violation Detection in Multi-Cloud Environment Using Hyperledger Fabric Blockchain. In *Proceedings of the 2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Nitte, India, 19 November 2021*; IEEE: Piscataway, NJ, USA, 2021; pp. 107–112.
53. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.