Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Blockchain for Distributed Systems Security in Cloud Computing: A Review of Applications and Challenges

Jawaher Abdulwahab Fadhil [1], Subhi R. M. Zeebaree[2]
jawaher.fadhil@auas.edu.krd[1], subhi.rafeeq@dpu.edu.krd[2]
[1] Department of Information Technology, Technical College of Informatics- Akre, Akre University for Applied Science, Duhok, Kurdistan Region, Iraq.
[2] Energy Eng. Dept., Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq.

Article Information

Submitted : 3 Mar 2024
Reviewed: 14 Mar 2024
Accepted : 1 Apr 2024

Keywords

Blockchain, Distributed Systems Security,Cloud Computing.

Abstract

The blockchain is a technology that utilizes a decentralized and distributed ledger system to enhance security in cloud computing for distributed systems. It has gained significant attention in various applications, including the Internet of Things (IoT) and cloud computing. However, the blockchain has scalability limitations that restrict its ability to handle different types of transactions effectively. On the other hand, cloud computing provides the availability of shared computer system resources on demand, but it faces challenges related to automation, process management, policy, and others. By combining blockchain technology with cloud computing in a unified system, it is possible to improve data integrity, resource management, pricing, fair compensation, and resource allocation. This article examines the applications and challenges of blockchain, emphasizing how it ensures data integrity, transparency, and resistance to tampering. It also explores various use cases to address obstacles like scalability issues and interoperability concerns, providing a comprehensive overview of the intersection between blockchain, distributed systems, and cloud computing security. The integration of cloud computing and blockchain is important for business applications because it offers advantages in terms of privacy, security, and service support. This review provides an extensive and up-to-date summary of the integration of cloud computing and blockchain, highlighting its significance in business contexts.

A. Introduction

Cloud computing provides computing services, including servers, storage, databases, networks, software, analytics, and information over the Internet, to achieve faster innovation, adaptable resources, and economies of scale [1]. Cloud computing consists of front-end and back-end. The backend consists of servers, computers, databases, and central servers. At the same time, the front-end allows users to access data stored in the cloud through a web browser or cloud computing software [2]. The main element in cloud computing that oversees the secure storage of data and information is called the backend. Cloud computing offers several advantages. These benefits include affordability, scalability, and accessibility of services [3] . In terms of accessibility, cloud computing improves mobility because most cloud services are self-service and available on demand. By accessing your documents from anywhere in the world without having to carry them with you, employees can access your documents from different locations [4]. It enables companies to quickly and efficiently scale up or down their IT departments in response to changing business needs. It is economical as it reduces the cost of purchasing and maintaining the equipment. Additionally, because we leverage the knowledge of the cloud provider's employees, we do not require a large IT team to manage your cloud data center operations [5]. Although cloud computing has many advantages, such as fast software upgrades, few maintenance problems, reliable data, and low cost, it poses a major challenge to the security of stored data. Blockchain technology is a way to solve cloud computing security issues. Blockchain was originally developed for trading Bitcoin; its applications extend far beyond cryptocurrencies. Blockchain is a trustworthy, hard-to-hack record of transactions. Although the technology is still new, it has revolutionary potential [6]. It is based on shared ledger technology, which uses a peer-to-peer network to securely store information. Blockchain ledgers can store a variety of data, including inventories, identities, logistics credits, land titles, and virtually any valuable information. The data is visible to all parties, and they can accept or reject it using consensus technology. Ensure that data is captured as a collection of "blocks" in a ledger and maintained in an immutable "chain" of time. Additionally, blockchain technology is integrated with a variety of metaheuristic (MA) algorithms. Currently, the MA algorithm has been applied in various fields such as mechanical engineering , civil engineering and energy, big data, and cloud computing [7]. For example, the Salp Swarm Optimization algorithm is integrated into the blockchain to solve routing problems in wireless sensor networks [8]. proposed an approach to solving the traveling salesman problem using blockchain and particle swarm optimization. In the field of medical computing, we proposed a service quality improvement method based on a novel MA algorithm and blockchain smart contract concepts. Distributed ledgers define three key characteristics [9]. Documentation is initially performed by storing the timestamp of the data. Second, the trading book is accessible to everyone and is therefore transparent. Third, the ledger is distributed in multiple places, and blockchain technology can help secure it [10]. Additionally, blockchain is difficult to attack due to its sharing and encryption capabilities, this is encouraging for IoT and business security [11]. Enterprise systems play a clear role in market processes, especially e-commerce systems, which play a fundamental role in today's world. With the development of technology, many new technologies have emerged that can serve e-commerce trends, such as the Internet of Things (IoT). Cloud computing and virtual market engineering to facilitate common e-commerce tasks in enterprise systems, such as: easily purchasing products, quickly providing services to customers, responding to customer inquiries online at an effective cost, etc. [12].However, in view of the rapidly changing market in a volatile environment and with increasing pressure from stakeholders, it is critical for companies to adopt a high degree of flexibility in competitive matters. Semantic Web (SW) technology plays an important role in search engines solving this problem by providing a way to understand the contextual meaning of data to retrieve relevant, high-quality results. An Exploratory Search System (ESS) is a specialized data discovery and retrieval method that helps searchers learn and explore topics and search goals that are unclear to them through a series of operations. For high-quality retrieval of ESS, Linked Open Data (LOD) is the best option [13]. Complex problems take longer to solve, and efficiency and performance are lower. Therefore, also To overcome these shortcomings, research has turned to methods that decompose the problem into independent domains. Divide and process each part separately so that each processing element can perform its part along with other issues. A parallel processor is a computer system composed of multiple processors. Processing units are connected via an interconnection network, as is the software required for processing [14]. All units work together. There are three types of parallel processing; shared, distributed, and hybrid storage systems. This article discusses a distributed storage system based on the client/server principle in the network Can contain any number of nodes; one of them is the client and the others are servers. The algorithm used here Ability to calculate (start, finish, consumed CPU, and total execution time and CPU). Server and client CPU (usage) and total execution time. There are many techniques for analyzing the performance of distributed systems [15]. However, one of the most commonly used technologies is Hadoop. It is an open-source software application framework that distributes storage and manages processes for big data applications running on clustered systems. However, it represents the center of a foundational growing system for advanced analytics, data mining, predictive analytics, and big data learning application technologies in distributed systems [16]. These companies are moving to cloud-based HR systems because HR data is huge and needs to be stored and accessed easily. The cloud is an excellent technology approach that can help companies stay competitive in a rapidly changing environment [17]. The other type of threat is information security in enterprise systems. Building a secure system for a company is a challenging task that requires the installation and deployment of features like encryption, integrity, and access control on the computer system [18]. These technologies represent a portion of the solution; the remaining portion must be provided. business environment security architecture, which includes an in-depth analysis of procedures, policies, and technology security [19]. High-performance field-programmable gate array (FPGA) devices enable parallel computing by building parallel processing elements (PEs) called virtual processors. One important reason is that FPGAs are specialized devices. Therefore, even if the parallel processing methods of PCs are applied, implementing systems based on these devices will yield faster and more accurate results than using PCs. In this paper, two high-performance computing (HPC) systems based on FPGA devices are developed [20]. One of the key characteristics of extended data is complexity. Heterogeneous data helps with data integration and big data processing problems. Both are essential but difficult to visualize and interpret in large databases because they require significant data processing and storage capacity. In the data age, where data is growing exponentially, extracting data in a way that the human brain can understand [21]. Cache coherence protocols play an important role in maintaining cache connectivity in multiprocessor environments [22]. The field of parallel processing involves methods used to improve the performance or other properties (e.g., cost-effectiveness, reliability) of digital computers through various forms of parallelism [23]. Centralized machines, known as "mainframe computers," which are centralized and utilized for computation, are able to perform multiple computation functions involving several clients in very timely planning. Eventually, the personal computer (PC) was released, which allows clients to execute their applications on demand with no need to wait for the mainframe scheduler to run their programs. As a result, PCs slowly declined, although the importance of mainframes is compelling, becoming more and more powerful [24]. Even though modern PCs have faster processors, they are still lagging behind in terms of size and remote sensing. Data sets increase due to higher-resolution sensors and larger research areas. A single workstation can not enough to handle these large amounts of data. The utilization of multiple processing cores in microprocessor architecture has changed as a result of advancements in the computer industry. The change allows one device to carry out multiple instructions simultaneously [25].

B. Methodology

To collect information on published papers, various sources such as IEEE Xplore, Google Scholar, SciSpace, and Springer were utilized. These platforms are widely used by researchers. The search terms employed included blockchain technology, security, and cloud computing. Additionally, references cited within the published works were examined to further supplement the research. After conducting a thorough review of these papers, it was observed that there were several studies directly addressing the topic of blockchain and its association with cloud computing security. A total of 20 peer-reviewed papers relevant to this research were identified. The publications were categorized and summarized in Table 1, which presents the challenges, techniques, and outcomes discussed in each study. The methodology for implementing blockchain in cloud computing for enhanced security in distributed systems encompasses several key steps.The following provides an overview of this methodology:

- Identify Security Requirements: To initiate the process, start by recognizing the precise security needs of the distributed system operating in the cloud. This entails comprehending the possible risks, weaknesses, and intended security goals. Take into account elements like data integrity, authentication, access control, auditing, and resilience.

- Evaluate Blockchain Suitability: Evaluate the appropriateness of utilizing blockchain technology to fulfill security requirements. Assess whether the attributes of blockchain, such as decentralization, immutability, and transparency, align with the desired security needs. Take into consideration factors such as scalability, performance, and compatibility with existing systems.
- Design Blockchain Architecture: Create a blockchain architecture that is compatible with both a distributed system and a cloud environment. Decide whether a public, private, or consortium blockchain is required for the specific use case. Establish the consensus mechanism, identity management protocols, and data storage models. Take into account the trade-offs between decentralization and performance when making these design choices.
- Integrate Blockchain and Cloud Infrastructure: Incorporate blockchain technology into the current cloud infrastructure and devise a plan for deploying and connecting blockchain nodes within the cloud environment. This may entail deploying blockchain nodes on virtual machines or containers and setting up the required network connectivity.
- Set up Identity Management: Implement a robust system for managing identities within the blockchain network. This involves tasks such as user authentication, authorization, and the issuance of digital identities. Consider employing cryptographic techniques, like public-private key pairs, to enhance security and safeguard user identities.
- Configure Security Measures: Configure additional security measures around the blockchain and cloud infrastructure. This may entail implementing encryption mechanisms, access controls, firewalls, and intrusion detection systems. Regularly monitor and update security configurations to address emerging threats.
- Conduct Testing and Auditing: Perform comprehensive testing and security audits of the blockchain implementation in the cloud environment. Test the system for vulnerabilities, conduct penetration testing, and validate the effectiveness of security measures. Conduct regular audits to ensure compliance with security policies and regulations.
- Educate Users and Establish Policies: Provide education to users and stakeholders about the security features, advantages, and proper usage of the blockchain-based distributed system. Establish clear security policies and guidelines to govern user behavior, data handling practices, and incident response procedures.
- Monitor and Update: Continuously monitor the blockchain-based distributed system for security incidents, anomalies, and emerging threats. Regularly review and update security measures as necessary.

C. Background Theory

1. Cloud Computing

Currently, cloud computing is a widely discussed subject in the field of information technology. With the distribution of computing resources such as servers, storage, databases, networking, software, and analytics, ensuring security becomes crucial. In these systems, the primary focus of security applications typically revolves around the following aspects:

1.1 IoT security

Hackers are increasingly exploiting edge devices like thermostats and routers to gain unauthorized access to networks in general. The rise of artificial intelligence (AI) has made it even easier for hackers to infiltrate entire systems, such as home automation, through "smart" switches and similar edge devices. In many cases, the security features of IoT devices are inadequate or incomplete [1]. The Internet of Drones (IoDT) has emerged as a popular research area, utilizing drones for data collection from terrestrial networks. This approach is being introduced to address issues such as congestion, safety concerns, and energy consumption in the Internet of Vehicles (IoV). The IoV faces challenges related to dynamic mobility, unsystematic traffic patterns, and degraded network performance in terms of latency, energy usage, and overhead costs. Furthermore, there is a potential for various attackers to disrupt traffic patterns [26].

1.2 DNS and DDoS security

A distributed denial of service (DDoS) attack is a form of assault that obstructs a user's access to a specific resource or service, such as a network resource, server, or website. These attacks have the potential to severely disrupt or slow down the targeted networks. Conversely, the highly centralized nature of the Domain Name System (DNS) makes it an attractive target for hackers aiming to exploit the connection between IP addresses and website names. Such an attack can render a website unusable, lead to financial losses, or even redirect users to fraudulent websites. Fortunately, blockchain technology can be utilized to decentralize DNS records and mitigate these types of attacks. By implementing blockchain, vulnerable single points of vulnerability that hackers exploit can be replaced with decentralized and more secure solutions [27].

1.3 Blockchain use cases in cybersecurity

While blockchain is not impervious to breaches, it has emerged as one of the most secure forms of digital network transactions. Its design and implementation aim to guarantee the integrity of information, and when utilized strategically, it can bring numerous benefits to various industries. Blockchain finds applicability across a wide range of applications and serves multiple purposes. One particularly impactful application is the integration of cybersecurity solutions with various other technologies, showcasing its potential in enhancing overall security measures.

1.4 Private messaging security

The increasing popularity of social media, as the internet connects people worldwide, has led to a rise in the number of social media platforms. These interactions generate a significant amount of metadata. Unfortunately, many users tend to use weak passwords to protect their accounts and the associated data. To address this concern, numerous messaging companies are adopting blockchain technology as a more effective alternative to existing end-to-end encryption methods for safeguarding username data. Blockchain can be utilized to establish fundamental security protocols and centralized API systems that facilitate cross-message communication capabilities. Recent incidents of attacks on prominent social media sites like Twitter and Facebook have resulted in widespread data breaches, compromising millions of accounts and exposing user data to unauthorized individuals. However, if implemented correctly within these messaging networks, blockchain technology has the potential to thwart potential cyberattacks, providing enhanced security measures.

1.5 Decentralized media storage

The increasing incidents of hacks and data theft are posing significant challenges for organizations. Many businesses still rely on centralized storage methods, which create a single point of weakness that hackers can exploit to gain access to the entire dataset. Such attacks compromise sensitive and confidential information, including crucial company financial data. To address this issue, blockchain technology offers a solution by introducing a decentralized form of data storage. This approach makes it more challenging for hackers to penetrate data storage systems, providing enhanced security for confidential information. As a result, numerous storage companies are actively exploring how blockchain can be leveraged to protect data from potential hackers.

1.6 Blockchain: The future of cloud computing

Blockchain-based cloud computing offers not just decentralized data storage but also finds increasing utilization in data logistics platforms. This technology allows multiple authorized users to simultaneously access, communicate, interpret, and modify data according to their needs. Cloud computing solutions powered by blockchain enable secure virtual analysis and management of knowledge. Furthermore, blockchain can virtualize contract transactions and other exchanges, leading to widespread adoption across various industries [28]. In the future, blockchain is poised to replace traditional cloud computing due to its ability to ensure robust information security. Data stored on the blockchain is not only stored in multiple nodes worldwide but is also highly distributed, addressing concerns regarding data security in the event of errors or faults in stored information. Moreover, all parties possessing the information hold the keys to access the encrypted data. While anyone can access the file, they can only access a portion of it, rendering it useless to unauthorized individuals. Given these advantages, blockchain technology is highly likely to become the prevailing choice [29].

2. Blockchain

Blockchain technology has garnered significant attention from various sectors, including finance, healthcare, utilities, real estate, and government agencies. It offers a wide range of applications, such as claims processing, identity management, operational visibility, auditing, supply chain security against counterfeit products, and ensuring data integrity from Internet of Things (IoT) devices. Blockchain is a distributed and fault-tolerant shared database that operates without central control, allowing all network users to participate. It is specifically designed to withstand attacks from compromised adversaries in highly competitive environments. By leveraging the computing power of honest nodes, blockchain invalidates opponents' strategies and makes information exchange resistant to manipulation and destruction. It also promotes the development of trusted networks within trusted environments [30].

The fundamental premise of blockchain is that applications can operate in a decentralized manner without relying on a trusted central authority. This enables the exchange of information among distrustful entities, even when the communication channel may have been compromised by external or internal parties. The absence of a central authority or intermediary accelerates the coordination process between entities. Manipulating blockchain is extremely challenging due to the use of encrypted data structures and the absence of single points of failure. Blockchain networks are fault-tolerant, allowing compromised nodes to be eliminated [31].

Blockchain is a decentralized and distributed ledger technology that securely records and verifies transactions across a network of computers. It consists of a chain of blocks, each containing a list of transactions. Once a block is completed, it is linked to the previous one, forming an immutable and chronological chain. The technology is widely recognized for its transparency, security, and resistance to tampering, making it valuable in various scenarios such as cryptocurrency transactions, supply chain management, smart contracts, enhancing security in distributed systems, and cloud computing [32].

Additionally, blockchain can be utilized to ensure the integrity of distributed copies of databases by storing crucial information about database transactions that cannot be discarded. It also enables fully distributed data control associated with databases. Gaetani et al. proposed a blockchain-based approach to enhance the security of distributed databases, particularly within the framework of Federation-as-a-Service (FaaS), which guarantees the production and management of cloud services and data [33]. In this approach, database interfaces in the cloud handle database-related issues. Operations are registered in the first phase of the blockchain using appropriate evidence and then executed on distributed database replicas. The blockchain is permissioned in the first phase, with each cloud member having a single miner. Miners use public and private keys to identify messages and achieve consensus through a mining rotation strategy that selects one miner as the leader within time-based periods. The miner leader receives new transactions, tags them with a key, and distributes them to other miners. Each miner's operation is added to the blockchain upon completion [35]. The second layer employs a blockchain anchoring method based on Proof of Work (PoW). Through time-based anchoring technology, operations in the first layer can be linked to blocks in the second layer [35].

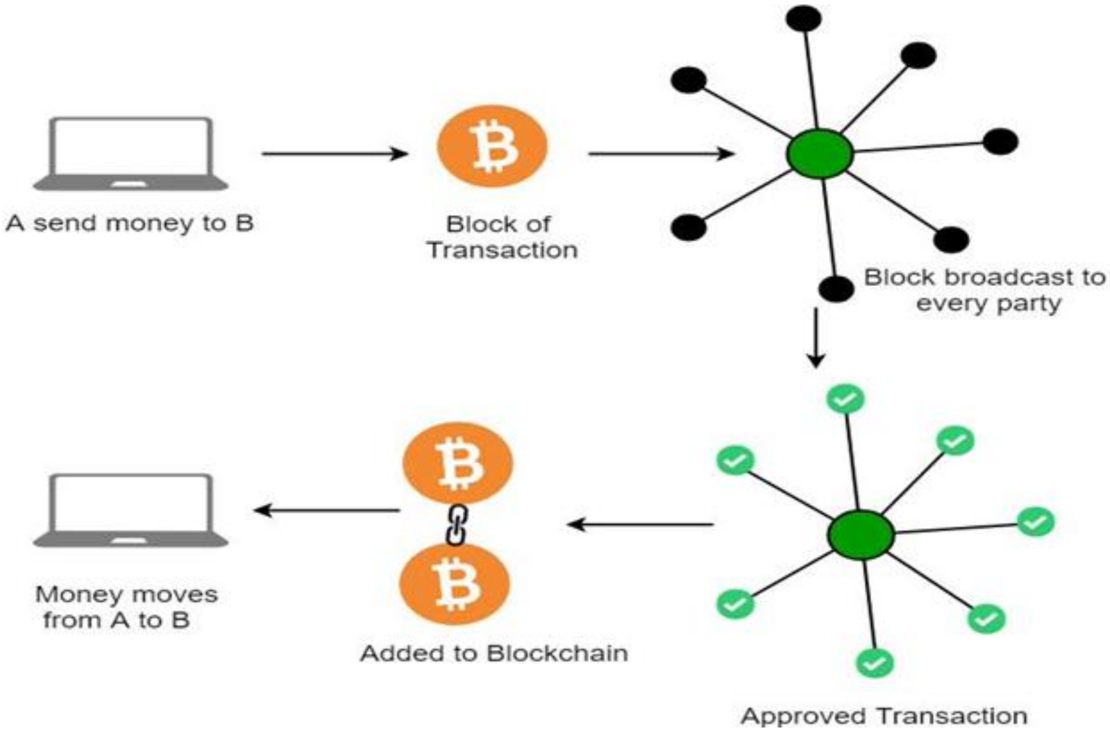

Figure 1. Blockchain and the future of the internet [36].

2.1 Blockchain Concepts

Blockchain technology incentivizes users to update the ledger and ensure its integrity during the processing of new transactions. Moreover, users can manage relevant information associated with each leader. By employing peer-to-peer communication, blockchain eliminates the need for costly third-party authorization in peer-to-peer transactions. The widespread availability of transaction information makes it more difficult to hack, ensuring speed, reducing security costs, and facilitating automatic approval and recording of transactions. The system can be easily connected, expanded, and deployed through open-source software. Additionally, transaction records are transparent and publicly viewable, leading to reduced regulatory costs. Blockchain technology combines peer-to-peer networks with distributed consensus methods to address the synchronization challenges of distributed databases [37]. Essentially, a blockchain is a distributed database that serves as an immutable public record of digital transactions. It operates as a distributed digital ledger, with each block in the chain identified by a cryptographic signature [36]. The fundamental principle of blockchain is decentralization, wherein data management occurs in a distributed manner, making data modification highly challenging [38]. Blockchain technology can be categorized into three main types:

- Public blockchain: In a public blockchain, anyone can verify transactions, confirm transactions, and participate in the consensus-building process. Examples of public blockchains include Ethereum and Bitcoin.

- Consortium chain: Consortium chains allow pre-selected authoritative nodes, typically used in business-to-business relationships, and can be considered partially decentralized. R3CEV and Hyperledger are examples of consortium chains.

- Private blockchain: In a private blockchain, the number of participating nodes is limited, and strict permission management rules govern data access. Regardless of the type, each blockchain offers its own advantages.

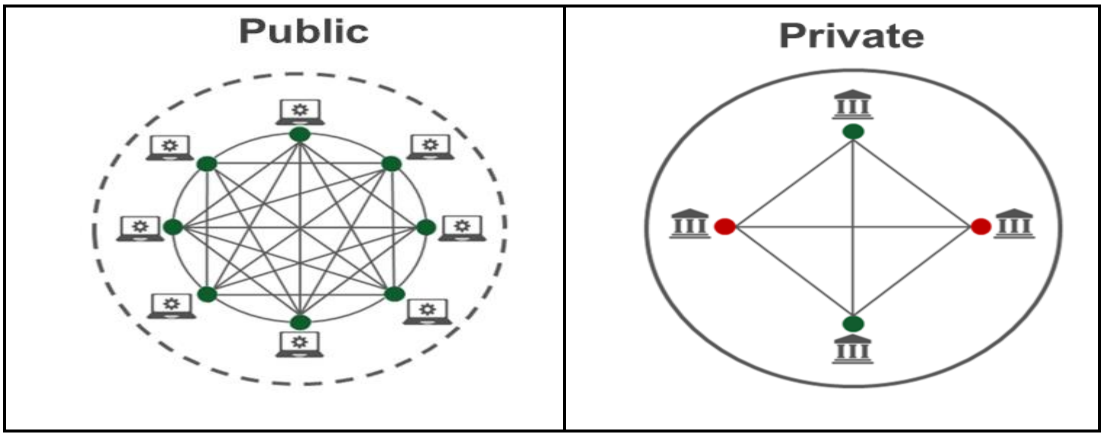

Figure 2. Private and Public Blockchain Network [39].

In terms of safety, the difference between a public and a private blockchain cannot be overstated. Because public blockchains are public, anyone can join and validate transactions on them. Moreover, only a small number of private blockchains are in use; commercial networks primarily employ them. A single corporation, or consortium, controls the membership [39].

2.2 Benefits of Blockchain technology in Cloud computing

One of the concerning developments in the realm of cloud computing is the growing adoption of blockchain technology. Many businesses rely on cloud storage and utilize cloud technologies extensively. When the power of blockchain is integrated into this combination, it holds the potential to bring about a revolutionary transformation across various industries. While cryptocurrencies, which utilize blockchain technology, tend to attract the most media attention, it is important to recognize that blockchain's impact extends far beyond just digital currencies [40].

2.3 Growth of Cloud Computing

The significant growth of the cloud can be attributed to its scalability, affordability, and flexibility. Organizations are increasingly adopting cloud services to streamline operations, facilitate collaboration, and enhance overall efficiency. The cloud serves as a platform for storing, processing, and accessing data, enabling businesses to quickly adapt to changing requirements. Advancements in technology, the rising volume of data being generated, and the demand for on-demand resources are key drivers behind this adoption. As cloud services mature, there is a growing emphasis on security, compliance, and the integration of emerging technologies like AI and edge computing [41]. In 2021, the percentage of global IT spending dedicated to the cloud continues to rise at an accelerated pace. The increasing utilization of blockchain technology in cloud computing is a particularly concerning trend. Many companies rely on cloud storage and leverage cloud technology extensively. By incorporating the power of blockchain into this mix, there is the potential for revolutionary changes across entire industries. While blockchain technology is commonly associated with cryptocurrencies, which receive significant media attention, its importance in cloud computing goes beyond that. Blockchain has the capacity to transform large-scale data processing and document capabilities in a cost-effective and stable manner, making it particularly significant in cloud computing practices.

2.4 Blockchain-based Security Solutions

Blockchain-based security solutions have gained significant attention and recognition due to their ability to provide decentralized and tamper-resistant systems. The immutability of blockchain ensures the integrity of data, making it highly secure. In the field of cybersecurity, blockchain technology is utilized for various tasks such as securing transactions, verifying identities, and protecting sensitive information. One notable feature of blockchain is the presence of smart contracts, which automate and enforce security protocols, reducing the risk of human error [42]. The transparency inherent in blockchain contributes to enhanced trust in security systems. Cryptocurrencies, which are built on blockchain technology, leverage cryptographic principles to facilitate secure financial transactions. As the technology continues to evolve, its application in securing different domains, including supply chains, healthcare, and Internet of Things (IoT) devices, continues to expand. However, despite its promising potential, challenges such as scalability and regulatory considerations remain areas of ongoing development and discussion. The diagram highlights the contributions of various cloud-based solutions, including aspects such as confidentiality, integrity, and availability (CIA), data verification, authenticity, cost-effectiveness, high performance, trust enhancement, deadlock management, functional solutions, data security enhancement, validity, and complexity. Here are four examples of blockchain-based security solutions:

- **Immutable Data Storage**

Blockchain offers a decentralized and unchangeable record-keeping system that ensures secure storage of data. By dispersing data across numerous nodes in a network, it becomes highly challenging for malicious individuals to tamper with or manipulate the information. This characteristic proves especially valuable when it comes to storing sensitive data like financial records, medical information, and identity documents.

- **Smart Contracts**

Smart contracts are coded agreements that automatically execute predefined actions when specific conditions are met. By leveraging blockchain technology, these contracts enhance security by eliminating the need for intermediaries and reducing the risk of fraud or manipulation. The decentralized nature of blockchain ensures that smart contract transactions are transparent, traceable, and resistant to tampering.

- **Supply Chain Security**

Supply chain security can be improved through the use of blockchain. By enabling end-to-end tracking and verification of products or goods, blockchain enhances the security and transparency of supply chains. Each step of the supply chain, from sourcing raw materials to final delivery, can be recorded on the blockchain, creating an auditable and tamper-proof history. This helps prevent counterfeiting, fraud, and unauthorized modifications within the supply chain.

- **Identity Management**

Identity management can also benefit from blockchain technology. Blockchain-based identity management solutions aim to provide secure and decentralized digital identities. Instead of relying on centralized authorities for authentication, blockchain enables users to have greater control over their identities. By storing identity information on a blockchain, users can selectively disclose their data for verification without revealing unnecessary personal details. This approach enhances privacy and reduces the risk of identity theft or data breaches. It is important to note that while blockchain technology offers significant security benefits, it should be implemented alongside other security measures to create a robust security framework. Additionally, the successful adoption of blockchain-based security solutions depends on factors such as scalability, interoperability, and regulatory considerations [43].

2.5 Blockchain applications for security of distributed systems in cloud computing:

Blockchain technology offers several key features that can enhance the security of distributed systems in cloud computing [44]:

- Immutable and Tamper-Proof Record-Keeping: The distributed ledger of blockchain ensures that data, once recorded, cannot be altered or tampered with without consensus from network participants. This feature can be leveraged to maintain an immutable record of system events, providing transparency and accountability for activities such as access logs, configuration changes, and software updates.

- Decentralization and Consensus: By implementing a blockchain-based consensus mechanism, such as proof-of-work or proof-of-stake, decision-making processes in distributed systems can be decentralized. This reduces the risk of a single point of failure or malicious attacks, as consensus is achieved through the agreement of multiple nodes in the network.

- Identity and Access Management: Blockchain can enhance identity and access management (IAM) in distributed systems by providing a decentralized and secure mechanism for user authentication and authorization. Blockchain-based identity solutions empower users to have control over their digital identities, reducing reliance on centralized identity providers and mitigating the risk of data breaches.

- Secure Data Sharing and Auditing: Blockchain facilitates secure data sharing and auditing in distributed systems. Encrypted data can be stored on the blockchain, and access control can be enforced through smart contracts, ensuring that data is shared only with authorized parties. The transparent nature of the blockchain enables efficient auditing and verification of data integrity.
- Fault Tolerance and Data Replication: Data redundancy and fault tolerance are crucial in cloud computing for system reliability and availability. Blockchain's distributed nature allows for data replication across multiple nodes, reducing the risk of data loss or system failure. Even if some nodes become unavailable or compromised, the data remains accessible from other nodes in the network.
- Smart Contracts for Automated Security Measures: Smart contracts, which are self-executing contracts with predefined rules and conditions, can automate security measures in distributed systems. They can enforce access control policies, trigger security protocols in response to specific events, and facilitate secure and auditable transactions between system components.

D. Literature Review on Security Applications in Blockchain

The objective of this paper [45] is to address data security concerns in cloud storage and propose a comprehensive strategy for cloud storage security. The authors highlight the significant issue of data theft, data leakage, and attacks on cloud data through the internet [46]. The survey focuses on analyzing and comparing various challenges in the cloud environment and security issues, with a specific emphasis on utilizing blockchain technology. Security in cloud computing is crucial as data transmitted over the internet requires robust mechanisms for data protection, including integrity, accountability, privacy, access control, authentication, and authorization. Blockchain technology offers solutions to overcome security challenges in cloud computing. Another study [47] examines security issues from different perspectives, providing a concise review of infrastructure and data-level security challenges, and delving into the concept of identity and access control in the cloud. Additionally, the paper discusses various approaches to mitigate or prevent security issues in a cloud environment. In a different work [48], the authors propose a secure digital evidence framework called Block-DEF, which utilizes blockchain technology with a loosely coupled structure. In this framework, evidence and evidentiary information are stored separately, with only evidence information being stored in the blockchain while evidence itself is stored on a trusted storage platform. To address blockchain bloating, the paper presents a lightweight blockchain that combines a hybrid block architecture with an improved name-based Byzantine fault-tolerance consensus mechanism. Furthermore, multi-signature technology is employed for evidence submission and retrieval. Analytical and experimental results demonstrate that Block-DEF is a scalable framework that ensures evidence integrity and authenticity while effectively balancing privacy and traceability. In another study [49], the authors analyze and compare the trust-enabling features of prominent blockchain oracle methods, technologies, and platforms. They also discuss research challenges that need to be addressed to ensure secure and reliable blockchain oracles. Despite the decentralized and trustless nature of blockchain systems, smart contracts alone cannot access data from the external world. Instead, smart contracts interact with external off-chain data sources called oracles, which are responsible for collecting and providing data feeds and inputs to smart contracts. However, there is always a risk associated with the data provided by an Oracle, as it may be corrupted, malicious, or inaccurate. The objective of this study [50] is to ensure that data stored in cloud storage is free from malware before it is accessed by end users. The paper proposes a popular malware detection strategy to enhance the security of cloud storage systems, particularly for high-risk data. This technique involves predicting data popularity and prioritizing data objects during time-consuming malware detection processes. By doing so, it helps prevent malware when frequently accessed data is involved. To address these concerns, a novel architecture is proposed in [51], which integrates multiple entities such as public clouds, a private cloud, smart contracts, and the data owner, client, or user. This decentralized cloud architecture establishes secure connections through smart contracts between the data owner and the private cloud, as well as between the client and the data owner. This approach ensures data protection against unauthorized access while providing users with a flexible and scalable solution for managing their data in the cloud. With this architecture, businesses and individuals can benefit from cloud-based storage while maintaining a high level of security and peace of mind. The paper [52] introduces a malware detection strategy that takes into account data popularity to enhance the security of cloud storage systems, particularly for high-risk data. By prioritizing popular data objects, which are expected to be frequently accessed, for malware detection, the proposed technique ensures the protection of high-risk data. It helps prevent malware when clients frequently access popular data by giving priority to malware detection for such data based on estimated popularity. In [53], the BCOT model is examined in various applied scenarios, including the integration of blockchain with supply chain management applications, challenges in combining blockchain with the cloud and IoT, and potential research directions. The study discusses the involvement of blockchain in supply chain management applications, the challenges associated with integrating blockchain with the cloud and IoT, and potential areas for further research. The application of blockchain technology in decentralized cloud storage is explored, highlighting its contributions to system security and credibility. In this investigation [54], the current and potential applications of blockchain technology in enterprise security systems are examined. The study aims to utilize modern blockchain technology to enhance cybersecurity in large corporations, considering the urgency of addressing cyber fraud committed by hackers and even company personnel. The authors propose a dynamic, blockchain-based model for the company's cybersecurity system. This modeling tool enables the creation of an effective computer model of a complex cybersecurity system, facilitating the design of the suggested improvements. The study [55] investigates how blockchains can address cloud computing challenges from legal and technical perspectives. It explores the utilization of blockchain in existing cloud storage applications and discusses its potential for resolving security and privacy issues. The paper examines how blockchain technology can be applied to enhance privacy and security in cloud computing. In [56], the challenges and limitations of cloud computing are evaluated, and blockchains are proposed as a solution. The authors discuss the utilization of blockchain technology in current cloud storage applications to address security and privacy challenges. The decentralized nature of blockchains enables consensus among users without relying on a central integration point, offering a novel form of distributed software architecture. The paper [57] introduces an innovative architecture that integrates multiple entities, including multiple public clouds, a private cloud, smart contracts, and the data owner, client, or user. This decentralized cloud architecture incorporates smart contracts between the data owner and the private cloud, as well as between the client and the data owner. This paper [58] explores the emerging technologies of blockchain and artificial intelligence (AI) and their potential impacts across various fields. It emphasizes the disruptive nature of blockchain technology in automating payments, providing secure access to shared data, and enabling direct interactions without intermediaries. Additionally, it highlights the cognitive capabilities of AI in learning, inferring, and adapting based on data.

In [59], a blockchain-based technique for ensuring data integrity authentication is introduced. The research aims to enhance secure operations, particularly in authentication processes involving users. By leveraging blockchain technology, the study aims to strengthen cloud security and mitigate potential threats and attacks. The paper utilizes the cuckoo filter and MHT to improve authentication and prevent unauthorized access to data in cloud storage units. The methodology is validated through various performance measures such as processing time, uploading time, downloading time, authentication time, consensus time waiting, and storage overhead. The proposed method is compared to traditional cloud security methods, demonstrating its superiority in enhancing cloud protection. The results validate the effectiveness of the proposed method, representing a significant advancement in cloud computing security.

In [60], the study discusses different approaches to ensure the security and confidentiality of user data. It also explores future strategies for cloud security. Cloud computing not only presents opportunities for saving resources but also transforms the way users engage with digital and mobile applications. The paper addresses precautions related to client and hardware authentication, information and resource access management, and data confidentiality. Concerns about cloud computing security are raised, considering the potential vulnerabilities such as unauthorized access to personal data and the risk of controlling sensitive information. Encryption algorithms are utilized to maintain data privacy during transmission, ensuring that only authorized users can decrypt the data. The Advanced Encryption Standard (AES) is commonly used for symmetric encryption and is well-known for its effectiveness. Various risks and dangers associated with data access and exploitation are discussed to promote a comprehensive understanding of the security landscape.

In [62], a blockchain-based access control scheme for mobile cloud computing is proposed to address privacy concerns. The scheme employs smart contracts to dynamically update access rights without incurring additional computing costs during authentication. It optimizes storage efficiency by recording a user's access rights across service providers in a single blockchain transaction. Mobile users can register once and access various providers using the same credentials. Security analysis confirms the scheme's safety, and communication costs are compared favorably to related schemes, highlighting its potential for privacy, efficiency, and scalability in mobile cloud computing.

In [63], a blockchain-based cloud environment data storage scheme is proposed to provide users with decentralized identity authentication and data integrity verification functions. Transaction information related to data storage is stored on the blockchain to ensure secure data storage. The paper addresses security risks associated with cloud storage, such as identity forgery, data theft, and privacy breaches. By leveraging blockchain technology, elliptic curve cryptography, and other techniques, the proposed scheme aims to enhance data security in cloud environments.

Lastly, in [64], a novel blockchain-based secure access framework (BSAF) is proposed for collaborations between cloud and device services with privacy protection. The framework utilizes a key matrix encryption mechanism to safeguard user behavior privacy and employs fully homomorphic encryption to protect the privacy of service content. Two smart contracts are designed: a request verification smart contract to verify user access rights and a behavior punishment smart contract to audit user access behaviors. Comprehensive experiments conducted on the Ethereum blockchain network demonstrate that the proposed BSAF framework outperforms existing schemes in terms of latency reduction, cost savings, and suitability for low-profile IoT devices..

E. Discussion and Comparison

The literature review section titled "Blockchain for Distributed Systems Security in Cloud Computing" offers a thorough examination of the reviewed sources in this field. The discussed references provide insights into how blockchain technology can enhance security within cloud computing environments. Multiple studies emphasize the decentralized nature of blockchain as a means to combat single points of failure and data breaches. The reviewed sources also highlight the immutability and transparency of blockchain, which can contribute to the integrity and auditability of cloud-based systems. Moreover, the literature investigates the utilization of smart contracts and consensus mechanisms in blockchain-based solutions for ensuring security in distributed systems. The findings collectively support the idea that blockchain holds promise in addressing security challenges in cloud computing and facilitating the development of more resilient and trustworthy distributed systems.

Table 1. Summary of previous studies used for Blockchain applications.

Reference	***Challenge***	***Algorithm and Analyzing Tools***	***Techniques***	***Description***	***Key Findings***
[45] Gajmal et al.,2018	The big data is stored on the internet	Virtualization for distributed computing	PDP	Discusses information security aspects for Data	It analyzes the security risks of user data in cloud storage and proposes a security technology based on the structural characteristics of cloud storage systems.
[46] Prathibha et al.,2019	Solutions can be developed to address challenges such as data security, data management, compliance, and reliability.	Blockchain technology is identified as a solution to overcome security issues in cloud computing .	Blockchain technique	Finds Blockchain overcomes the security issues in cloud computing.	analyzing and comparing various issues in the cloud environment and security issues using blockchain
[47] Mujawar et al.,2019	The security issues exist in context of infrastructure, data and storage, access control in cloud environment.	Explores various security issues in cloud computing, including infrastructure , data, and access control, and discusses different solutions to alleviate these issues.	Not explicitly mention specific techniques for cloud computing security.	the security issues at infrastructure level, data level, and also discusses the concept of Identity and Access Control in cloud.	the different solutions to avoid or alleviate the security issues in cloud environment are discussed.
[48] Tian et al.,2019	Guarantees the integrity and validity of evidence, and balances privacy and traceability well.	The multi-signature technique is adopted for evidence submission	(Block-DEF)	Tolerance consensus mechanism is proposed to avoid blockchain bloat.	The performance of Block-DEF is analyzed and evaluated through simulation, experiments.
[49] Salah et al.,2020	Provides integrity, authenticity, and confidentiality to stored data.	Tabulate, and summarize the emerging blockchain applications, platforms,	Blockchain technologies for (AI)	The applications discuss AI and blockchain technology and their	Blockchain technology has the ability to automate payment in cryptocurrency and to provide access to a shared ledger of data, transactions, and logs

		and protocols specifically targeting AI area.		integration into different systems	in a decentralized, secure, and trusted manner.
[50] Peng et al.,2020	Conducive to keeping malware at bay when popular data are frequently accessed by clients.	Development of cutting-edge of cloud storage systems	Malware detection techniques	A means of prioritizing data objects amid malware detection procedures	Our technique is conducive to keeping malware at bay when popular data are frequently accessed by clients.
[51] You Tsai et al.,2020	There are two functions: anonymous file sharing and searches to find illegally downloaded files	The pure blockchain and the traditional database.	Using square chain technology, multiple tags and mysterious encrypted information streams	Anonymity and immutability of blockchain to enhance security.	Cloud users can access data through smart contracts, recognize all users within the application layer.
[52] Nahar et al.,2021	avoids many attacking challenges and single point of failure.	system of cryptography	algorithm technique with a private key from a user.	guarantees data of the security and credibility of the system.	Data retention, secure decentralized cloud storage, system data authenticity.
[53] Maesaroh et al.,2022	Information system that uses blockchain technology.	Blockchain-based system dynamic model of the company's cybersecurity system.	Blockchain technology	Address the problem of enhancing the degree of cybersecurity.	The increased system response in cases of employee fraud.
[54] Naje.,2022	Provides integrity, authenticity, and confidentiality to stored data.	Distributed Ledger Technology (DLT) and various cryptographic algorithms.	(DLT)	The paper analyzes the root cause of cloud security. attacks	Provides integrity, authenticity, and confidentiality to all stored data.
[55] Moslemzadeh et al.,2022	Use of blockchain in blockchains as a solution for each issue will be proposed by explaining how of cloud computing	Among the SLA issues is service	Blockchain technology can be used to resolve security	The use of blockchain technology in security issues in cloud computing.	The use of blockchains as a solution for each issue will be proposed by explaining how they can overcome the shortcomings of cloud computing.
[56] Rani et al.,2022	That basic security	The blockchain	The blockchain	A quick review of	The study is to investigate a quick

	concerns are properly addressed in different cloud regions.	innovation mechanism is the most important innovation behind Bitcoin.	innovation mechanism	previous reflections centered on blockchain integration.	review on earlier contemplations centred on blockchain joining with the cloud in order to display their amazingness as a research target.
[57] Adiga et al.,2023	Provides a robust form of security for data stored in the cloud infrastructure is susceptible to various types of vulnerabilities, threats, and attacks that can compromise its confidentiality, availability, and integrity.	Cloud-based storage over traditional on-premise storage	Cloud-based storage	The use of smart contracts helps ensure that data is protected. .	Providing users with a flexible, scalable solution to manage their data in the cloud, maintaining the highest levels of security , peace of mind.
[58] Abidin , 2023	Provides integrity, authenticity, and confidentiality to stored data.	The chain finance and supply	Blockchain technology	The work enhanced the security and integrity of cloud data.	Cloud data security, data management.
[59] Ramachandran et al., 2023	Validation using performance metrics like processing, uploading, downloading, authentication t, consensus, waiting, initialization time, and storage overhead.	Data integrity authentication using blockchain. The cuckoo filter and MHT used in the authentication process.	Data integrity and secure cloud operations blockchain technology. -Cuckoo filter and Merkle Hash Tree (MHT) to facilitate authentication process enhancement.	A blockchain-based technique for data integrity authentication. Use of cuckoo filter and MHT as methods to improve the authentication process.	The proposed approach helps efficiently secure operations and user authentication in cloud computing settings. It proves superior computational and storage performance relative to conventional approaches in cloud security.
[60] Basha et al.,2023	The future potential strategies for cloud security are examined.	Advanced Encryption Standard (AES) is the symmetric	(AES)	An overview on cloud security to understand the security	The data may be accessed and exploited in a variety of ways, and it is also critical to understand

		encryption algorithm that is more frequently utilised		concerns and solutions. the dangers.	
[61] Ramesh et al.,2023	User authentication can be provided by using the iris verification system and data confidentiality	The proposed system utilizes a hybrid cryptographic technique that combines AES, DES, and CST for data confidentiality.	Hybrid cryptographic technique	User authentication is achieved using the iris verification system.	Data retrieval and data integrity are ensured through the use of a data matrix code and a blockchain verification scheme.
[62] Yu et al.,2023	The security goal of our proposed scheme is to prevent privacy leakage during the blockchain-based access control process.	Distributed Mobile Cloud Computing (MCC) services	MCC	The data on the public ledger is blinded using Pedersen commitments	Performance analysis, computational efficiencies, superior communication, low storage capacity of blockchain
[63] Xiong.,2023	The traditional cloud trust model, which is centralized, can cause management overhead, network congestion, and single points of failure	Elliptic curve cryptography and other technologies,	Based on blockchain, elliptic curve cryptography and other technologies,	The scheme provides decentralized identity authentication and data integrity verification functions .	The transaction information of data storage is stored on the blockchain to ensure the safe storage of data
[64] Li Duan et al.,2023	protect IoT service contents.	BSAF	BSAF	The framework utilizes key matrix encryption	Protect privacy, reduce time, and save costs

F. Extracted Statistics

According to the chart, the distribution of challenges is as follows: 60% of the challenges pertain to securing data storage, with an emphasis on implementing encryption and protection measures against breaches. Another 10% of the challenges focus on safeguarding Internet of Things (IoT) devices. Privacy protection accounts for 20% of the challenges, which involves compliance with data protection regulations and ensuring the security of personally identifiable information. The remaining 10% of challenges are dedicated to ensuring secure access to data, which encompasses the implementation of authentication protocols and access controls. In summary, the challenges are spread across different areas, including securing data storage, protecting IoT devices, ensuring privacy, and enabling secure access to data, as depicted in Figure 3.

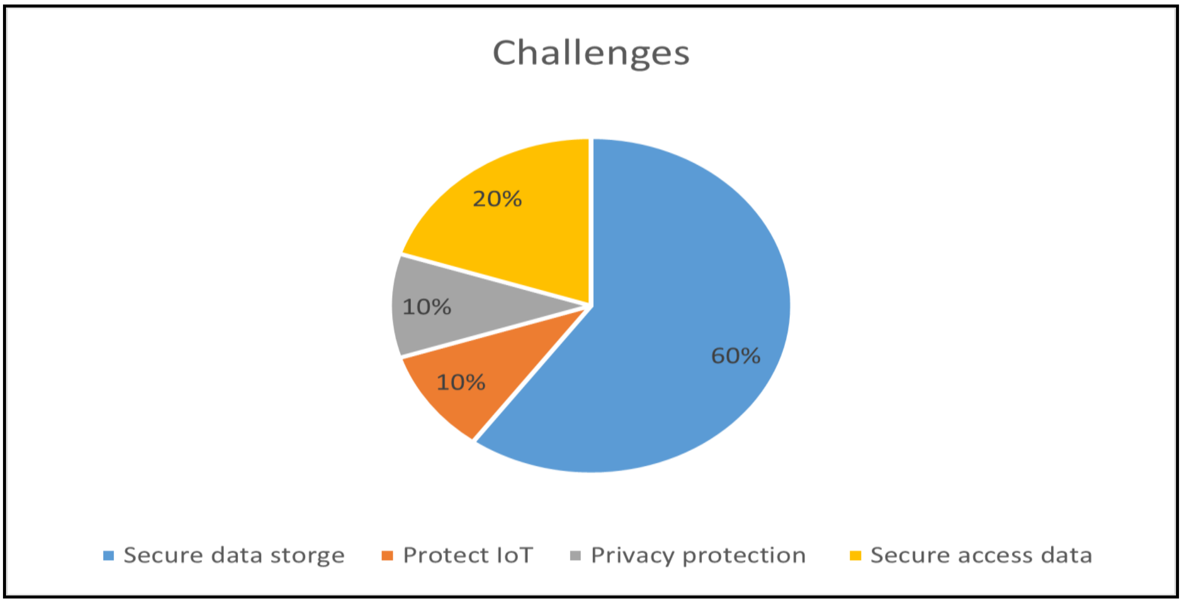

Figure 3. The challenges identified in per studies discussed in the table.

The chart illustrating cloud security techniques highlights several important measures. These measures include the implementation of Data Encryption Frameworks (DEF), such as the widely-used Advanced Encryption Standard (AES), which ensures secure storage and transmission of data. Additionally, Multi-Hash Techniques (MHT) play a role in maintaining data integrity and providing protection against unauthorized access. The chart specifically emphasizes the utilization of blockchain techniques, which leverage decentralized and tamper-resistant ledgers to enhance the security of cloud transactions and data. This involves employing blockchain for secure identity and access management, thereby establishing a transparent and unchangeable record of user permissions. In summary, the chart emphasizes the integration of DEF, MHT, and blockchain techniques as a multi-layered approach to strengthen cloud computing security. This approach ensures robust data protection, as depicted in Figure 4.

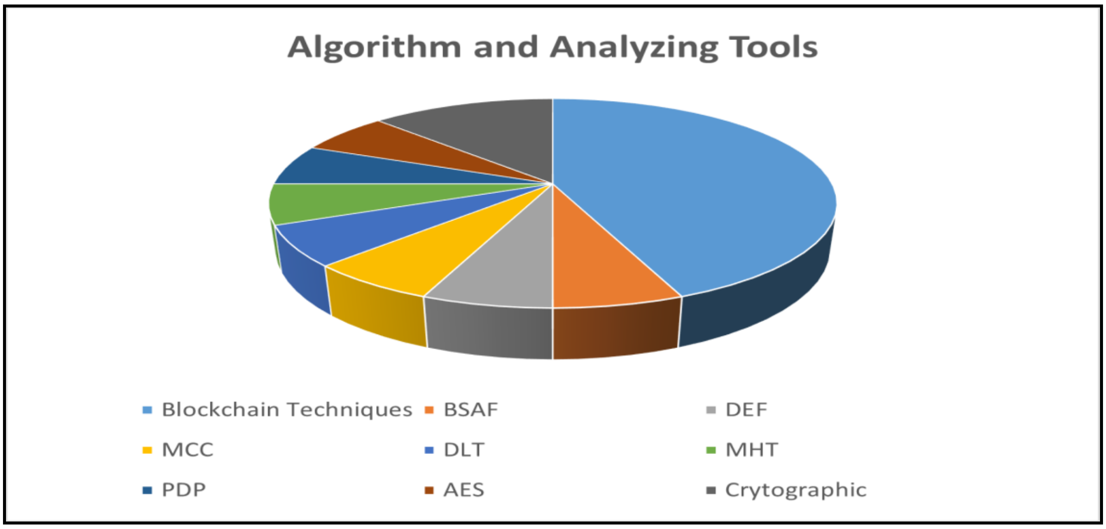

Figure 4. Approaches applied to secure cloud computing.

Blockchain technology offers a robust solution to mitigate the financial impact of data breaches on organizations. By utilizing blockchain, companies can proactively prevent breaches, avoiding the complex consequences of litigation, financial losses, compromised data, and the costly aftermath of security incidents. A significant portion of organizations' IT budgets, exceeding 20% according to [65], is allocated to strengthening security and data protection measures. Among these measures, a substantial portion is dedicated to combatting malware, which incurs an average annual cost of $2.4 million. Data breaches have far-reaching consequences that go beyond the initial incident, often requiring months of dedicated efforts to restore affected systems. Recent findings from a comprehensive report by IBM highlight the evolving financial landscape of data breaches, with costs reaching $3.2 million per year. This represents a significant 12% increase over the past five years, as depicted in Figure 5. This upward trend underscores the urgent need for innovative and effective solutions, positioning blockchain as a strategic investment for organizations to fortify themselves against the escalating financial impact of data breaches.

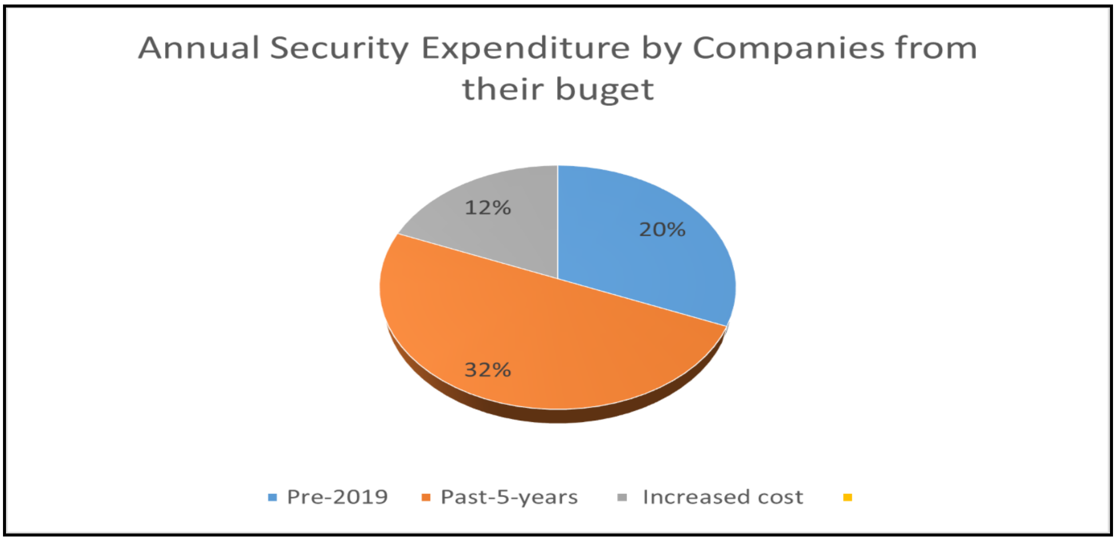

Figure 5: Annual security expenditure by companies from their budget.

At the same time, adversaries have reduced the average time it takes to carry out a ransomware attack. However, there is still significant potential for organizations to enhance their detection and response speeds, as nearly 40% of the organizations studied have not yet implemented security AI and automation.

Some organizations that were part of the study exhibit reluctance to involve law enforcement during a ransomware attack due to concerns that it may complicate the situation. The IBM report, for the first time this year, delved deeper into this issue and found evidence to the contrary. It was discovered that organizations that did not engage law enforcement experienced breach lifecycles that were, on average, 33 days longer compared to those that did involve law enforcement. Moreover, this silence came at a cost, as ransomware victims who did not involve law enforcement paid breach costs that were, on average, $470,000 higher than those who did involve law enforcement. Despite ongoing efforts by law enforcement to collaborate with ransomware victims, 37% of respondents still chose not to engage them. Additionally, almost half (47%) of the studied ransomware victims reportedly paid the ransom. It is evident that organizations should dispel these misconceptions surrounding ransomware. Paying a ransom and avoiding law enforcement may actually lead to increased incident costs and slower response times.

There has been some progress in threat detection and response. According to IBM's 2023 Threat Intelligence Index, defenders were able to stop a higher proportion of ransomware attacks last year. However, adversaries continue to find ways to evade defensive measures. The report revealed that only one in three breaches studied were detected by the organization's own security teams or tools, while 27% of breaches were disclosed by the attacker and 40% were disclosed by a neutral third party like law enforcement.

Organizations that discovered the breach themselves experienced breach costs nearly $1 million lower than those disclosed by the attacker ($5.23 million compared to $4.3 million). Breaches disclosed by the attacker also had a significantly longer lifecycle, approximately 80 days longer, compared to those identified internally (320 days versus 241 days). These findings highlight the substantial cost and time savings associated with early detection, demonstrating that investing in these strategies can yield long-term benefits.

G. Challenges and Recommendations

Blockchain technology, being a nascent innovation, encounters various issues and concerns that have been categorized into different challenges based on research and studies. It is widely recognized as a significant technological advancement and has garnered attention from numerous prominent companies. Over the past few years, the adoption of blockchain technology has gained significant traction [66].

1. **Blockchain-Cloud Integration Challenges:** Blockchain technology has emerged as a potential solution to tackle the security challenges faced by cloud computing. It is recognized as an immutable and transparent digital ledger that imparts integrity, authenticity, and confidentiality to stored data [67]. By combining blockchain and cloud computing, the security and privacy of distributed systems can be enhanced. Blockchain networks can be established within the framework of cloud security, making them well-suited for blockchain implementations. The inherent characteristics of blockchain, such as transparency, traceability, decentralization, and security, offer potential remedies for security issues in cloud applications [68]. Nonetheless, there exist obstacles and challenges to effectively integrating blockchain and cloud systems that require attention. Further research and improvements are necessary to explore various architectures, models, and roles of cloud computing in facilitating the integration of blockchain and cloud systems.

2. **Blockchain's Double-Edged Sword:** Blockchain technology offers a solution to tackle security challenges in cloud computing by introducing transparency, traceability, decentralization, security, immutability, and automation. While cloud computing is widely adopted, it still faces unresolved security issues [69]. By integrating blockchain, cloud data security can be enhanced, ensuring privacy and traceability of transactions. However, the integration of blockchain and cloud computing may lead to increased performance costs for cloud platforms [70]. The conventional centralized trust model of cloud computing can result in management overhead, network congestion, and single points of failure. In contrast, the decentralized framework and distributed computing paradigm of blockchain make it suitable for establishing a distributed and decentralized trust architecture within cloud computing systems.

3. **Cloud-Bound Challenges:** Integrating blockchain and cloud computing presents challenges, including the absence of transparency and traceability in evaluating trust, necessitating further research in this domain. However, the integration of blockchain and the cloud enables the development of solutions to tackle issues such as data security, data management, compliance, and reliability.

4. **Redesigning Blockchain for Sensitive Environments:** A blockchain is an openly accessible public ledger, which is often necessary in various scenarios. However, in sensitive environments, this accessibility can pose a risk. Blockchain technology still has a considerable distance to go in terms of achieving widespread acceptance. To address this concern, the ledger needs to undergo redesigning to restrict access only to authorized individuals who have permission to view it [71].

5. **Blockchain's Promises and Pains in Value Transfer:** Blockchain technology is extensively employed in facilitating the value transfer process, aiming to minimize expenses linked with intermediaries and middlemen. Despite its numerous benefits, blockchain is still in its early stages and presents challenges when it comes to integration into current systems. Consequently, it remains inaccessible for the majority of businesses and governments [72].

6. IoT and Blockchain: The collaboration between human-machine interaction and machine-to-machine communication is frequently employed to empower intelligent workforces. Although IoT and blockchain technologies offer numerous notable benefits, they also come with certain drawbacks. These obstacles primarily arise from the imperative to address security and privacy concerns. Challenges such as interoperability, legal considerations, absence of standards, access control, regulatory issues, development hurdles, and the evolving economics of IoT represent just a few of the obstacles that must be overcome in the realm of IoT and blockchain technology [73].

H. Conclusion

In conclusion, blockchain technology holds the potential to enhance security within distributed systems in cloud computing environments. With its decentralized and transparent nature, blockchain can mitigate security risks associated with centralized systems by providing secure data storage and management. The distributed ledger of blockchain ensures that data, once recorded, cannot be altered or tampered with without consensus from network participants. Furthermore, blockchain can contribute to enhancing identity and access management (IAM) in distributed systems by offering a decentralized and secure mechanism for user authentication and authorization. This study presents a comprehensive survey of the integration of cloud computing and blockchain, highlighting its crucial role in enterprise applications due to its advantages in privacy, security, and service support. The paper begins by introducing the concept of blockchain and discussing its relevance to security concerns. It explores the benefits of incorporating blockchain technology into cloud computing and examines the growth of cloud computing in this context. The focus then shifts to various applications of blockchain for enhancing security, followed by a discussion of the main technical challenges in integrating blockchain and cloud computing. It is important to note that the implementation of blockchain in distributed systems necessitates careful consideration of scalability, performance, and interoperability factors. Additionally, the adoption of blockchain technology in cloud computing is an ongoing process, requiring organizations to assess specific requirements and trade-offs before integrating blockchain into their distributed systems.

REFERENCES

[1] A. Manzoor, W. Ahmad, M. Ehatisham-ul-Haq, A. Hannan,M. A. Khan, M.U. Ashraf, A. M. Alghamdi, A. S. Alfakeeh, “Inferring Emotion Tags from Object Images Using Convolutional Neural Network,” Applied Sciences, vol. 10, no. 15, p. 5333, Aug. 2020.

[2] H. M. Zangana and S. R. M. Zeebaree, “Distributed Systems for Artificial Intelligence in Cloud Computing: A Review of AI-Powered Applications and Services,” *International Journal of Informatics, Information System and Computer Engineering (INJIISCOM)*, vol. 5, no. 1, pp. 1–20, Jan. 2024, Accessed: Feb. 21, 2024.

[3] N. A. Kako, S. R. M. Zeebaree, M. A. M. Sadeeq, A. Alkhayyat, and H. M. Shukur, “DDLS: Distributed Deep Learning Systems: A Review,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. *12*(10), 7395-7407. 2021.

[4] H. S. Abdullah and S. R. M. Zeebaree, “Distributed Algorithms for Large-Scale Computing in Cloud Environments: A Review of Parallel and Distributed Processing,” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 15s, pp. 356–365, Feb. 2024, Accessed: Feb. 21, 2024.

[5] T. M. G. Sami, S. R. M. Zeebaree, and S. H. Ahmed, “A Comprehensive Review of Hashing Algorithm Optimization for IoT Devices,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 6s, pp. 205–231, May 2023, Accessed: Feb. 21, 2024.

[6] S. R. Zeebaree, A. B. Sallow, B. K. Hussan, & S. M. Ali.” Design and simulation of high-speed parallel/sequential simplified DES code breaking based on FPGA”. In *2019 International Conference on Advanced Science and Engineering (ICOASE)*. IEEE, p. 76-81, 2019.

[7] Z. M. Khalid, S. R. M. Zeebaree, "Big Data Analysis for Data Visualization: A Review," International Journal of Science and Business, IJSAB International, vol. 5(2), pages 64-75,2021.

[8] S. M. Mohammed, K. Jacksi, and S. R. M. Zeebaree, “A state-of-the-art survey on semantic similarity for document clustering using GloVe and density-based algorithms,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, pp. 552–562, Apr. 2021.

[9] S. R. Zeebaree, & K. Jacksi. “Effects of processes forcing on CPU and total execution-time using multiprocessor shared memory system”. International Journal Of Computer Engineering In Research Trends, vol. *2*(4), 275-279, 2015.

[10] S. R. Zeebaree, L. M. Haji, I. Rashid, R. R. Zebari, O. M. Ahmed, K. Jacksi, & H. M. Shukur. “Multicomputer multicore system influence on maximum multi-processes execution time”. *TEST Engineering & Management*, vol. *83*(03), pp.14921-14931, 2020.

[11] Y. S. Jghef, M. J. M. Jasim, H. M. Ghanimi, A. D. Algarni, N. F. Soliman, W. El-Shafai, S. R. M. Zeebaree, A. Alkhayyat, A. S. Abosinnee, N. F. Abdulsattar, A. H. Abbas, H.M. Hariz & F. H. Abbas, “Bio-Inspired Dynamic Trust and Congestion-Aware Zone-Based Secured Internet of Drone Things (SIoDT). *Drones*, vol. *6*(11), 337, 2022.

[12] M. A. Sadeeq, & S. R. Zeebaree. “ Design and implementation of an energy management system based on distributed IoT” . *Computers and Electrical Engineering*, vol. *109*, pp.108775, 2023.

[13] H. Malallah, S. R. Zeebaree, R. R. Zebari, M. A. Sadeeq, Z. S. Ageed, I. M. Ibrahim, K. J. Merceedi, “A Comprehensive Study of Kernel (Issues and Concepts) in Different Operating Systems,” *Asian Journal of Research in Computer Science*, vol. 8, no. 3, pp. 16–31, May 2021.

[14] S. R. M. Zeebaree, “DES encryption and decryption algorithm implementation based on FPGA,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 774–781, 2020.

[15] L. M. Haji, S. R. M. Zeebaree, K. Jacksi, and D. Q. Zeebaree, “A State of Art Survey for OS Performance Improvement,” *Science Journal of University of Zakho*, vol. 6, no. 3, pp. 118–123, Sep. 2018.

[16] S. M. Mohammed, K. Jacksi, & S. R. Zeebaree,” A state-of-the-art survey on semantic similarity for document clustering using GloVe and density-based algorithms”. *Indonesian Journal of Electrical Engineering and Computer Science*, vol. *22*(1), pp. 552-562, 2021.

[17] H. Fawzia, D. Ahmeda, S. A. Mostafac, M. F. M. Fudzeec, M. A. Mahmoodd, S. R. Zeebaree, & D. A. Ibrahimf, "A Review Of Automated Decision Support Techniques For Improving Tillage Operations", *REVISTA AUS*, vol. *26*, pp. 219-240, 2019.

[18] B. S. Osanaiye, A. R. Ahmad, S. A. Mostafa, M. A. Mohammed, H. Mahdin, R.S. Subhi, & O. I. Obaid, "Network data analyser and support vector machine for network intrusion detection of attack type". *REVISTA AUS*, vol. *26*(1), pp. 91-104, 2019.

[19] I. M. I. Zebari, S. R. M. Zeebaree, and H. M. Yasin, "Real Time Video Streaming From Multi-Source Using Client-Server for Video Distribution,", In *2019 4th Scientific International Conference Najaf (SICN). IEEE Xplore*, pp. 109-114, Apr. 01, 2019.

[20] A. H. Ibrahem and S. R. M. Zeebaree, "Tackling the Challenges of Distributed Data Management in Cloud Computing - A Review of Approaches and Solutions," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 15s, pp. 340–355, Feb. 2024.

[21] S. R. M Zeebaree and I. M. I Zebari, "Multilevel Client/Server Peer-to-Peer Video Broadcasting System," *Article in International Journal of Scientific and Engineering Research*, vol. 5, no. 8, 2014.

[22] H. Shukur, S. Zeebaree, R. Zebari, O. Ahmed, L. Haji, and D. Abdulqader, "Cache Coherence Protocols in Distributed Systems," *Journal of Applied Science and Technology Trends*, vol. 1, no. 3, pp. 92–97, Jun., 2020.

[23] D. A. Hasan, K. Hussan, S. R. M. Zeebaree, D. M. Ahmed, O. S. Kareem, and M. A. M. Sadeeq, "The Impact of Test Case Generation Methods on the Software Performance: A Review," *International Journal of Science and Business*, vol. *5*(6), pp. 33-44. 2021.

[24] N. Cavus, D. A. M. Zebari, and S. R. M. Zeebaree, "*Digital Logic Circuits Reduction: A Binary Decision Diagram Based Approach,"*. LAP LAMBERT Academic Publishing, 2016.

[25] I. M. Ibrahim, S. R. Zeebaree, H. M. Yasin, M. A. Sadeeq, H. M. Shukur, & A. Alkhayyat, "Hybrid Client/Server Peer to Peer Multitier Video Streaming". In *2021 International Conference on Advanced Computer Applications (ACA),* IEEE., (pp. 84-89). July, 2021.

[26] M. Ashraf, M. Shah, and I. Ilyas, "A Survey on Data Security in Cloud Computing Using Blockchain: Challenges, Existing State of the Art Methods, and Future Directions." *Lahore Garrison University Research Journal of Computer Science and Information Technology*,vol. *5*(3), pp.15-30, 2021.

[27] H. Musa, M. Krichen, A. A. Altun, and M. Ammi, "Survey on Blockchain-Based Data Storage Security for Android Mobile Applications," *Sensors*, vol. 23, no. 21, pp. 8749–8749, Oct. 2023.

[28] K. Prathapchandran, & P. Rutravigneshwaran. "Trust Based Security Mechanisms for Resource-Constrained Internet of Things-A Review". In *Journal of Physics: Conference Series* (Vol. 1850, No. 1, p. 012042). IOP Publishing. May, 2021.

[29] Y. Liu, K. Qian, K. Wang, & L. He," Effective scaling of blockchain beyond consensus innovations and moore's law: Challenges and opportunities". *IEEE Systems Journal*, vol.*16*(1), pp. 1424-1435, 2021.

[30] J. Kaur Chahal, A. Bhandari, and S. Behal, "Distributed Denial of Service Attacks: A Threat or Challenge," *New Review of Information Networking*, vol. 24, no. 1, pp. 31–103, Jan. 2019.

[31] I. S. Abdulkhaleq, & S. R. Zeebaree. "State of Art for Distributed Databases: Faster Data Access, processing, Growth Facilitation and Improved Communications", International Journal of Science and Business, vol. *5*(3), pp. 126-136, 2021.

[32] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, & D. Mohaisen. " Exploring the attack surface of blockchain: A comprehensive survey ". *IEEE Communications Surveys & Tutorials*, vol. *22*(3),pp. 1977-2008, 2020.

[33] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, "Denial-of-Service Attack on IEC 61850-Based Substation Automation System: A Crucial Cyber Threat towards Smart Substation Pathways," *Sensors*, vol. 21, no. 19, p. 6415, Sep. 2021.

[34] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, & N. Kumar, " Blockchain data-based cloud data integrity protection mechanism". *Future Generation Computer Systems*, vol.*102*, pp. 902-911, 2020.

[35] M. Mitre, B. J. Marlin, J. K. Schiavo, E. Morina, S. E. Norden, T. A. Hackett, C. J. Aoki,and M. V. Chao, "A Distributed Network for Social Cognition Enriched for Oxytocin Receptors," *Journal of Neuroscience*, vol. 36, no. 8, pp. 2517–2535, Feb. 2016.

[36] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-Voting System Based on Blockchain Technology: A Survey," In *2021 International Conference on Information Technology (ICIT)*, IEEE., (pp. 200-205), 2021.

[37] L. Ismail and H. Materwala, "Article A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 11, no. 10, p. 1198, Sep. 2019.

[38] J. Gong and N. J. Navimipour, "An in-depth and systematic literature review on the blockchain-based approaches for cloud computing," *Cluster Computing*,vol. *25*(1), pp. 383-400, 2022.

[39] K. Godawatte, P. Branch, & J. But, "Use of blockchain in health sensor networks to secure information integrity and accountability". *Procedia Computer Science.* vol. 210, pp.124-132, 2022.

[40] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, Jul. 2019.

[41] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain Meets Cloud Computing: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 1, no. 2, pp. 1–1, 2020.

[42] J. Park and J. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions," *Symmetry*, vol. 9, no. 8, p. 164, Aug. 2017.

[43] M. R. Dorsala, V. N. Sastry, and S. Chapram, "Blockchain-based solutions for cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 196, p. 103246, Dec. 2021.

[44] R. Awadallah and A. Samsudin, "Using Blockchain in Cloud Computing to Enhance Relational Database Security," *IEEE Access*, vol. 9, pp. 137353–137366, 2021.

[45] A. Albassam, F. Almutairi, N. Majoun, R. Althukair, Z. Alturaiki, A. Rahman,& M. Mahmud, "Integration of Blockchain and Cloud Computing in Telemedicine and Healthcare". *IJCSNS*, vol. *23*(6), pp. 17-26, 2023.

[46] L. Duan, W. Xu, W. Ni, and W. Wang, "BSAF: A blockchain-based secure access framework with privacy protection for cloud-device service collaborations," *Journal of Systems Architecture*, vol. 140, p. 102897, Jul. 2023.

[47] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, Jul. 2019.

[48] N. Nahar, F. Hasin, & K. A. Taher, "Application of Blockchain for the Security of Decentralized Cloud Computing". In *2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD),* IEEE. pp. 336-340, February ,2021.

[49] Y. Zhang, L. Xiong, F. Li, X. Niu, and H. Wu, "A blockchain-based privacy-preserving auditable authentication scheme with hierarchical access control for mobile cloud computing," *Journal of Systems Architecture*, vol. 142, p. 102949, Sep. 2023.

[50] S. Maesaroh, H. J. Permana, P. Dirgayusa Febrianaga, Noviyanti, and R. A. Pardosi, "Blockchain Technology in the Future of Enterprise Security System from Cybercrime," *Blockchain Frontier Technology*, vol. 2, no. 1, pp. 1–8, Jun. 2022.

[51] I. A. Naje, V. K. Shukla, D. Gupta, & D. B. Ojha, "Addressing Cloud Security Challenges through Blockchain Technology". In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-6). 2022.

[52] P. M. Tehrani, G. Kotsis, & A. R. Pranata, "Blockchain Technology for Addressing Privacy and Security Issues in Cloud Computing". In International Conference on Cyber Warfare and Security ,Vol. 17, No. 1, pp. 194-200. , March, 2022.

[53] S. Veena, C. J. Tejas Mallikarjun, S. Vishwesh Adiga, C. Venkatesh, and P. D. Yogish, "Cloud Security Using The Smart Contracts," In International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES). IEEE, pp. 312-316, 2023.

[54] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[55] W. Y. Tsai, T. C. Chou, J. L. Chen, Y. W. Ma, and C. J. Huang, "Blockchain as a Platform for Secure Cloud Computing Services," 22nd International Conference on Advanced Communication Technology (ICACT). IEEE, p. 155-158, 2020.

[56] M. Rani, Kalpna Guleria, and Surya Narayan Panda, "Blockchain Technology Novel Prospective for Cloud Security," In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE. (pp. 1-6). 2022.

[57] A. Ramachandran, P. Ramadevi, A. Alkhayyat, and Y. K. Yousif, "Blockchain and Data Integrity Authentication Technique for Secure Cloud Environment," *Intelligent Automation & Soft Computing*, vol. 36, no. 2, pp. 2055–2070, 2023.

[58] X. Guo, Z. Xiong, J. Chen, & D. Chen. " A secure, blockchain-based data storage scheme for cloud environments". International Conference on Computer, Artificial Intelligence, and Control Engineering (CAICE 2023) (Vol. 12645, pp. 512-517), 2023.

[59] A. Ramachandran, P. Ramadevi, A. Alkhayyat, and Y. K. Yousif, "Blockchain and Data Integrity Authentication Technique for Secure Cloud Environment," Intelligent Automation And Soft Computing, vol. 36, no. 2, pp. 2055–2070, 2023.

[60] A. Markandey, P. Dhamdhere, and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," International Conference on Computing, Power and Communication Technologies (GUCON). IEEE, 2018. p. 633-636. 2018.

[61] S. M. Basha, V. Rishik, V. J. Krishna, and S. Kavitha, "Data Security in Cloud using Advanced Encryption Standard," In 2023 International Conference on Inventive Computation Technologies (ICICT)). IEEE. pp. 1108-1112, 2023.

[62] K. L. Neela, & R. K. Ramesh. "A Hybrid Cryptography Technique with Blockchain for Data Integrity and Confidentiality in Cloud Computing". In *Cloud Computing Enabled Big-Data Analytics in Wireless Ad-hoc Networks*, pp. 15-29. 2022.

[63] S. Pavithra, S. Ramya, and S. Prathibha, "A Survey On Cloud Security Issues And Blockchain," In 2019 3rd International Conference on Computing and Communications Technologies (ICCCT). IEEE, p. 136-140, 2019.

[64] L. B. Bhajantri and T. Mujawar, “A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures,” In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC),IEEE., (pp. 376-380), Dec. 2019.

[65] P. Sharma, D. M. Shukla, and A. Raj, “Blockchain adoption and firm performance: The contingent roles of intangible capital and environmental dynamism*,” International Journal of Production Economics, vol. 256, p. 108727, Feb. 2023.*

[66] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, “Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges,” *ACM Computing Surveys*, vol. 54, no. 8, pp. 1–36, Nov. 2022.

[67] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2521–2549, 2020.

[68] A. Khanna, A. Sah, V. Bolshev, A. Burgio, V. Panchenko, and M. Jasiński, “Blockchain–Cloud Integration: A Survey,” *Sensors*, vol. 22, no. 14, p. 5238, Jul. 2022.

[69] Ch. V. N. U. Bharathi Murthy, M. Lawanya Shri, S. Kadry, and S. Lim, “Blockchain Based Cloud Computing: Architecture And Research Challenges,” *IEEE access*, vol. *8*, pp. 205190-205205, 2020.

[70] Z. S. . Ageed and S. R. M. . Zeebaree, “Distributed Systems Meet Cloud Computing: A Review of Convergence and Integration”, *Int J Intell Syst Appl Eng*, vol. 12, no. 11s, pp. 469–490, Jan. 2024.

[71] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing,” *Future Internet*, vol. 14, no. 11, 2022.

[72] A. A. Sadawi, M. S. Hassan, and M. Ndiaye, “A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges,” *IEEE Access*, vol. 9, pp. 54478–54497, 2021.

[73] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018.