Journal of Theoretical and Applied Information Technology
31st January 2024. Vol.102. No 2
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BLOCKCHAIN-ENHANCED CYBERSECURITY AND PRIVACY IN CLOUD COMPUTING: A SYSTEMATIC LITERATURE REVIEW

ISHRAG HAMID[1] , MOUNIR FRIKHA[2]

[1,2] Department of Computer Networks & Communications.

King Faisal University, CCSIT , Al Hofuf, Al Hassa 31982, Saudi Arabia,

E-mail: [1] 223002631@student.kfu.edu.sa , [2] mmfrikha@kfu.edu.sa

ABSTRACT

This paper presents a comprehensive exploration of blockchain-based privacy and cybersecurity solutions for cloud computing. Recognizing blockchain's origins in the realm of digital currencies, the authors meticulously explore its evolution into a robust, decentralized, and cryptographic tool, capable of addressing the intricate challenges faced in cloud computing environments. The study is comprehensive, covering not only the theoretical aspects of blockchain technology but also its practical applications, which extend beyond the traditional boundaries of cloud computing to include areas like digital currencies, smart contracts, and supply chain management. The authors critically assess the opportunities and challenges that blockchain integration presents for cloud computing. They shed light on how blockchain's inherent properties – such as immutability, transparency, and cryptographic security can effectively mitigate common security threats and privacy concerns in cloud environments. The review also acknowledges the complexities involved in implementing blockchain technology, such as issues related to scalability, energy consumption, and the need for regulatory frameworks that can adapt to the decentralized nature of blockchain. In essence, this paper offers a holistic view of blockchain's role in cloud computing, striking a balance between its potential to revolutionize data security and the pragmatic challenges that need addressing for its widespread adoption. The authors' exploration opens new avenues for future research and development in the field, highlighting blockchain's growing importance in the evolving digital landscape.

Keywords: *Blockchain, Cloud Computing, Cybersecurity, Data Privacy, Decentralization, Data Integrity, Cryptographic Algorithms, Scalability*

1. INTRODUCTION

In the contemporary digital landscape, cloud computing has become a cornerstone for storing and processing vast amounts of data, offering scalability, flexibility, and cost-effectiveness [1]. However, this growing dependence on cloud services has raised significant concerns about privacy and cybersecurity [2]. Traditional security measures often struggle to address the sophisticated cyber threats and privacy issues inherent in cloud environments. Blockchain technology, characterized by its decentralized architecture and robust security mechanisms, presents a novel approach to mitigating these challenges [3]. This paper presents an exhaustive exploration of how blockchain technology, known for its foundational role in digital currencies, has evolved into a potent, decentralized, cryptographic solution adept at tackling the nuanced challenges of cloud computing. The paper navigates through the theoretical underpinnings and practical applications of blockchain, extending its scope beyond cloud computing to realms like digital currencies, smart contracts, and supply chain management.

This research does more than just highlight the transformative potential of blockchain in enhancing cloud computing security; it also meticulously examines the practical challenges associated with its integration, including scalability, energy consumption, and the need for adaptive regulatory frameworks. The paper's comprehensive review illuminates blockchain's inherent properties - immutability, transparency, and cryptographic security - and their role in effectively mitigating prevalent security threats and privacy concerns in cloud environments. Moreover, it acknowledges the complexities involved in implementing blockchain technology and underscores the importance of this paper in guiding future research and development in this field. It emphasizes the increasing significance of blockchain in the digital landscape, paving the way for its broader adoption while addressing the

practical challenges for its widespread implementation in cloud computing. The authors' thorough investigation and analysis serve as an essential resource for advancing understanding in both academic and industry contexts, influencing policy-making and practical applications in leveraging blockchain technology for bolstering cybersecurity and privacy in cloud computing environments.

2. PRISMA METHODOLOGY

PRISMA 2020 utilizes the model shown in Figure 1 as a guide to help us select and assess the articles that are related to our topic. 7540 research papers were found employing the search terms "Blockchain" and "Cloud Computing" and "Cybersecurity" and "Data Privacy" and "Data Integrity" or "Decentralization" or "Cryptographic Algorithms" or "Scalability" in the Saudi Digital Library and Google Scholar during the identification stage. There are still two thousand papers when duplication is removed. Various techniques might be employed to eliminate repetitions in the picked study articles. Sets, built-in functions, and iterative approaches are frequently utilized to eliminate redundant processes. In order to prevent data duplication, these techniques were utilized to eliminate duplicate searches and choose relevant research. Three thousand and five hundred forty papers were screened during the screening phase. One hundred papers omitted after perusing the subjects and abstract. Since the prior publication date had nothing to do with our topic, two hundred were disqualified. Fifty papers have met the requirements to move on to the final round during the eligibility stage Figure 1.

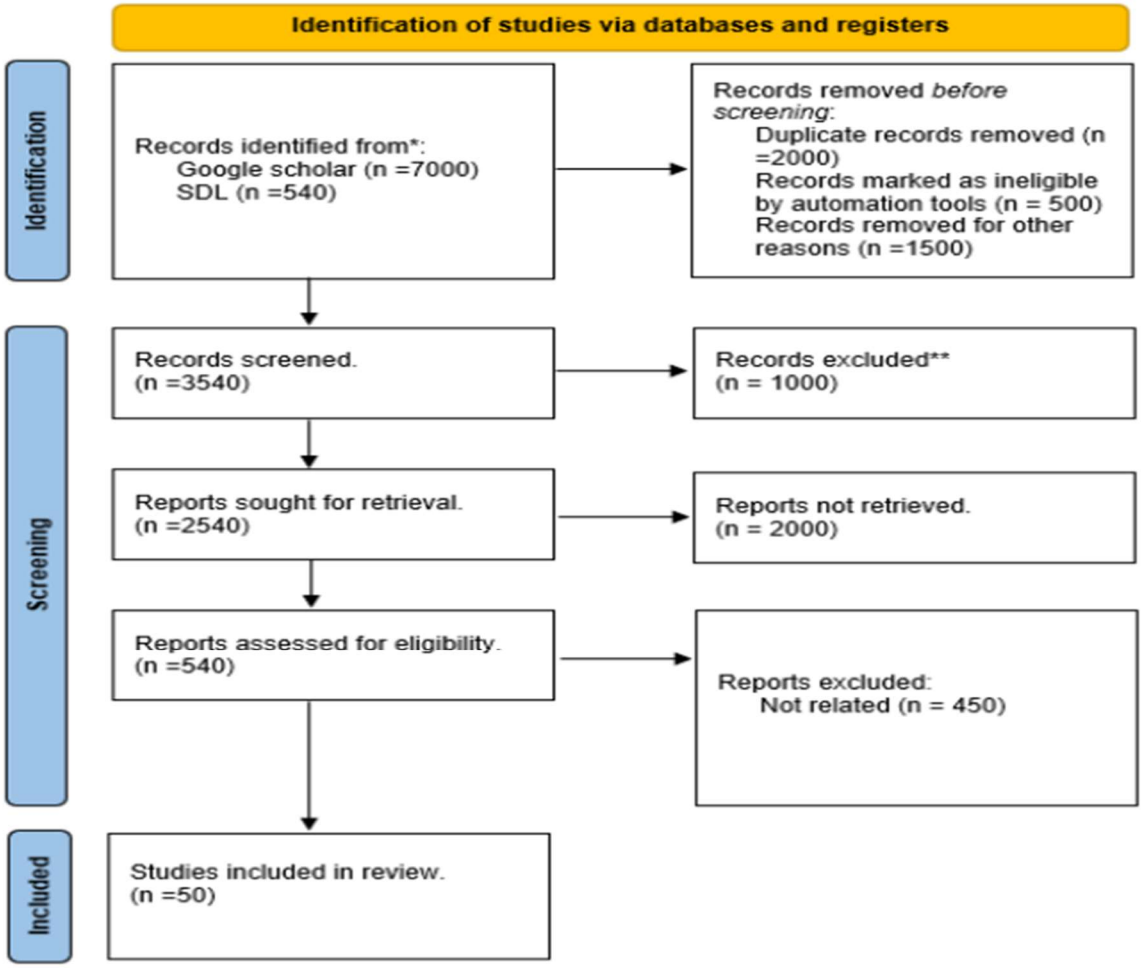

Figure 1: PRISMA Methodology

3. BLOCKCHAIN FOR CLOUD

The concept of blockchain was introduced as the underlying technology for Bitcoin. Satoshi Nakamoto's seminal paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," introduces Bitcoin, a revolutionary digital currency system that operates without the need for any centralized authority. The paper outlines a decentralized network using a blockchain, a public ledger of all transactions, maintained by a network of nodes. Key innovations include a proof-of-work mechanism to ensure network consensus and prevent double-spending, enabling secure, transparent, and tamper-resistant transactions. Nakamoto's work addresses common issues in digital currency, such as fraud and trust, by creating a system where trust is established not through a central entity but through a decentralized, cryptographic, and computational approach, paving the way for the future of digital currencies [4].

Figure 2 illustrates the concept of blockchain technology, it depicts interconnected blocks, each containing a unique hash code, transaction data, and the hash of the previous block, visually representing the chain of blocks. It also includes a depiction of a decentralized network of computers, emphasizing the security, transparency, and immutability characteristic of blockchain technology. Blockchain technology is distinguished by several key characteristics: it is decentralized, allowing for a consensus-driven approach among untrusted participants without the need for a central authority, which eliminates single points of failure [5]. It offers transparency, making records auditable and traceable. Its security is robust, utilizing cryptographic hash functions and private keys to protect records from tampering. A defining feature of blockchain is its immutability; once data is recorded, it cannot be altered without detection, thanks to the chaining of blocks and cryptographic hashes. These properties collectively make blockchain a powerful tool for secure, transparent, and reliable digital transactions [6].

Blockchain technology has diverse applications, including serving as the backbone for cryptocurrencies like Bitcoin, enabling automated and self-executing smart contracts, and enhancing supply chain transparency and traceability. It's used in secure digital voting systems, the management of healthcare records with improved privacy, and in banking for secure transactions and record-keeping. Blockchain also aids in protecting intellectual property rights and automating royalty payments for creators, and offers reliable solutions for identity verification, demonstrating its versatility across various industries even in cloud computing [7].

Cloud computing is a transformative technology that allows for the delivery of various services over the internet, such as storage, servers, databases, networking, software, and analytics. Characterized by its flexibility, scalability, and cost-effectiveness, it enables users and enterprises to access and store data remotely, eliminating the need for extensive physical infrastructure [8]. This technology supports a wide range of applications, from email and file sharing to complex data analysis and artificial intelligence operations. It offers on-demand services with pay-as-you-go pricing models, making it an efficient solution for businesses of all sizes. With its ability to rapidly scale resources based on demand, cloud computing is a cornerstone of modern IT infrastructure, driving innovation and digital transformation across various industries [9].

The integration of cloud computing presents significant security and privacy challenges, primarily due to the nature of data storage and management being handled off-site and over the internet. Key concerns include data breaches, where sensitive information may be accessed by unauthorized parties, and data loss, where critical data could be lost or corrupted. Privacy issues arise from the potential for unauthorized access and misuse of personal and confidential data stored on cloud servers. Furthermore, cloud environments are susceptible to various cyber threats, such as hacking, malware, and DDoS attacks [10].

The integration of blockchain and cloud computing offers significant benefits, including enhanced security through blockchain's decentralized and immutable nature, improved data integrity due to transparent and traceable data changes, and robust privacy protection mechanisms [11,12]. This integration reduces reliance on centralized control, thereby increasing system resilience and reducing single points of failure. Additionally, it offers greater transparency and traceability, facilitating compliance with regulatory requirements, and enables the potential for automated, secure transactions and agreements through smart contracts, thereby enhancing the efficiency and effectiveness of cloud computing services [13,14].

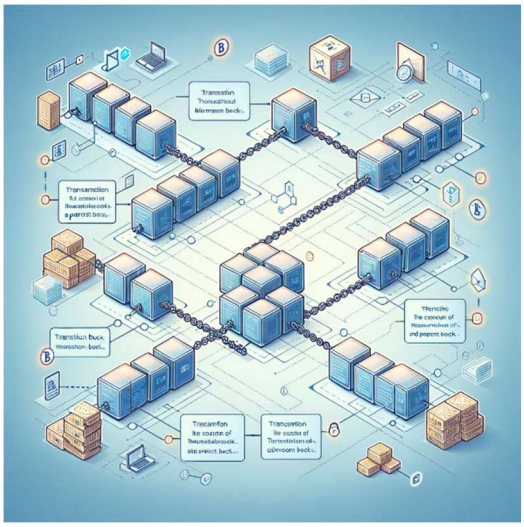

Figure 2. Blockchain Architecture Overview

4. RELATED WORK

This paper [15] proposes a new cloud data provenance architecture called ProvChain, which is decentralized and trustworthy. ProvChain is designed to collect and verify cloud data provenance by embedding the provenance data into blockchain transactions. Blockchain-based data provenance can provide tamper-proof records, enable the transparency of data accountability in the cloud, and help to enhance the privacy and availability of the provenance data. The paper provides an overview of data provenance and blockchain technology, and describes the design of ProvChain in detail. The architecture operates mainly in three phases: provenance data collection, provenance data storage, and finally provenance data validation. ProvChain provides security features including tamper-proof provenance, user privacy, and reliability with low overhead for the cloud storage applications. The paper presents a detailed implementation of ProvChain and evaluates its performance. The results from the performance evaluation demonstrate that ProvChain provides a secure and efficient way to collect and verify cloud data provenance. The paper concludes that ProvChain can be applied to other types of data units besides cloud files, and provides a promising solution for secure data provenance in cloud computing environments.

This paper [16] highlights blockchain technology as a secure solution for storing and sharing information through an immutable distributed ledger. The paper proposes a blockchain-based data provenance architecture, Block Cloud, incorporating a Proof-of-Stake (PoS) based consensus protocol, CloudPoS, to securely record data operations in the cloud. This protocol leverages cloud users' cyber infrastructure resources. The paper details the creation of a cloud-based testbed environment using a local cluster of physical machines managed by Xen hypervisor and Kubernetes for resource elasticity. Dockerized containers emulating peers in the Blockchain network were used for testing. The effectiveness of CloudPoS was evaluated in a simulated environment, and performance tests were conducted to assess the proposed consensus.

This paper [17] is about Blockchain Security in Cloud Computing. It provides an overview of blockchain technology and its research trends, as well as how to adapt blockchain security to cloud computing and its secure solutions in detail. It discusses the benefits of using blockchain technology in cloud computing, how it can enhance security, and the challenges associated with implementing blockchain security in cloud computing and how to address them.

This paper [18] proposes a blockchain-based EHR sharing scheme with conjunctive keyword searchable encryption and conditional proxy re-encryption to realize data security and privacy preservation of data sharing between different medical institutions. The paper discusses the key technologies, system architecture, threat model, security goals, data structure, consensus mechanism, protocol, security proof, computational overhead, and communication overhead. The authors evaluate the performance of the system by implementing it on the Ethereum platform. The paper concludes by summarizing the findings and looking ahead to the future.

This paper [19] is a comprehensive guide to AuthPrivacyChain, a blockchain-based access control framework with privacy protection in the cloud. The paper provides a detailed overview of the technology, including its key features, architecture, and security mechanisms. AuthPrivacyChain uses a decentralized and tamper-proof blockchain to store access control rights and uses blockchain account addresses as identities. The paper also discusses how AuthPrivacyChain encrypts and stores access control rights in the blockchain to protect user privacy. This paper proposes a scheme named Elliptical Curve Certificateless Aggregate Cryptography Signature (EC-ACS) for public verification and auditing in the Medical Cloud Server (MCS) to secure EHR using authorized blockchain technology. This scheme uses Elliptic

Curve Cryptography (ECC) to encrypt medical data and a Certificateless Aggregate Signature scheme (CAS) for digital signature generation, ensuring secure data sharing and storage in cloud storage. This approach promises enhanced security, privacy, and protection against unauthorized access in cloud health systems.

Pepper [20] resolving security and privacy challenges in blockchain technology requires a multifaceted approach. Firstly, robust consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) are crucial for preventing malicious actors from compromising the network's integrity. Strong cryptographic techniques, including encryption and digital signatures, should be employed to safeguard data confidentiality and authenticity. Smart contracts must undergo rigorous auditing to identify and rectify vulnerabilities that could be exploited. Ensuring the security of the underlying network infrastructure through measures like DDoS protection and secure communication channels is paramount. Permissioned blockchains can enhance security by limiting network access to authorized participants. Adherence to established security standards and best practices is essential in development and deployment. Bug bounties and security audits can incentivize the community to report vulnerabilities promptly. Privacy challenges can be addressed through techniques like zero-knowledge proofs and confidential transactions to protect sensitive information while maintaining data integrity. Regular software updates and patching help stay ahead of emerging threats. Lastly, user education and awareness play a vital role in mitigating security risks. This comprehensive approach encompasses technical, procedural, and human-centric aspects, contributing to a more secure and privacy-respecting blockchain ecosystem.

This paper [21] delves into how blockchain technology can fortify security and privacy across various applications, emphasizing its decentralized structure as a key factor in overcoming the vulnerabilities of centralized systems. This decentralization, combined with the strategic use of advanced cryptographic techniques, significantly enhances data security and user privacy. The paper also explores blockchain's role in specific sectors like smart grids, evaluating how its application can improve security and privacy in these areas. Furthermore, it provides an in-depth comparison of different consensus algorithms, which are fundamental to the functioning and security of blockchain networks. Alongside this, the paper highlights the critical role of smart contracts in blockchain, focusing on their security aspects to ensure reliable and secure transactions, ultimately proposing a comprehensive approach to leveraging blockchain for heightened security and privacy in various digital applications.

This paper [22] also focuses on introducing and comparing blockchain-based technologies to address various challenges in smart grids. These challenges include privacy protection, identity authentication, data aggregation, and electricity pricing, especially concerning the data collection and power energy trading processes in smart grids. The paper presents a comprehensive view of how blockchain technology can be leveraged to enhance the security and privacy aspects of modern smart grid systems.

Paper [23] addresses the issue of privacy for COVID-19 positive patients whose data are made public, leading to potential violations of rights and threats to their lives. It proposes a scheme using traditional ciphertext policy attribute-based encryption (CP-ABE) for enhanced security and fine-grained access control. However, this method puts a strain on resource-limited devices and poses a risk of privacy leakage. To counter these challenges, the paper introduces a verifiable ABE scheme that combines blockchain and local differential privacy (LDP). This approach perturbs data locally to resist collusion attacks, outsources encryption and decryption to reduce load on mobile terminals, and uses smart contracts for fair execution and preventing errors in semi-honest cloud servers. The proposed scheme is shown to be effective in protecting privacy, optimizing data accuracy, computational overhead, storage performance, and fairness, and is the first to apply LDP and blockchain in a tracing system, improving data accuracy and aiding in health prevention and control.

The authors in paper [24] explore the role of blockchain technology in addressing data privacy and security challenges in cloud computing environments. They propose a blockchain-based architecture that leverages the inherent features of blockchain, such as immutability and traceability, to ensure transparent and auditable processing of personal data. The proposed architecture involves four primary components: data owners who retain control over their personal data, service providers that handle personal data on behalf of data owners, data processors who process data on behalf of service providers, and a blockchain ledger that maintains audit trails of personal data processing

activities. To address concerns regarding scalability and performance, the authors suggest employing techniques such as data sharing and off-chain storage. Additionally, they advocate for the development of standardized data processing agreements and consent frameworks to facilitate seamless integration of blockchain-based personal data processing systems.

Paper [25] proposes a blockchain-based IAS (BC-IAS) protocol specifically for cloud computing. This protocol is designed to bolster security and privacy by incorporating decentralized key management, identity verification, and secure authentication. The focus is on addressing the inherent concerns around security and privacy in cloud computing environments, leveraging the strengths of blockchain technology to create a more secure and private cloud computing framework.

The paper [26] focuses on a blockchain-based system specifically designed for e-health, targeting the enhancement of security and confidentiality for patients' electronic health records (EHRs) in cloud environments. It addresses the critical need for robust data protection in healthcare, where sensitive patient information is often stored and accessed. By integrating blockchain technology, the proposed system aims to leverage its capabilities for secure transactions and data integrity to better safeguard EHRs against unauthorized access and breaches. This approach reflects a growing trend in healthcare to adopt advanced technologies like blockchain for improved data security and privacy.

Additionally, blockchain technology is employed to guarantee the integrity, traceability, and secure storage of medical records in the cloud environment. Table 1 shows summary of other related work.

5. DISCUSSION

Recent scholarship has explored cloud computing and blockchain technology, showing a convergence of efforts to improve data security and privacy across network platforms. Zhang et al. [22] discuss Blockchain's security and privacy risks in mobile cloud computing. The authors also suggest implementing a uniform authentication mechanism to reduce these concerns. Liang et al. [11] emphasize the importance of data provenance and suggest using ProvChain to create unalterable documentation and encourage transparency.

Wang et al. [14] examined cloud-based EHR security and privacy. The authors recommend a blockchain-based EHR sharing mechanism to protect data. Rajendran et al. [39] propose using blockchain technology to address internet privacy and security challenges. Esposito et al. [37] agree that cloud healthcare data safety is important. Yang et al. [15] present AuthPrivacyChain, a blockchain-based access control solution that mitigates centralized cloud computing vulnerabilities. Mohanta et al. [16] examine blockchain technology's applications and potential to improve privacy and security. Wen et al. [17] and Cao et al. [18] examine security monitoring in blockchain-based applications and smart grid systems, respectively, adding to the discussion. Qin et al. [19] evaluate COVID-19 patient tracing privacy. This concern could be addressed by combining blockchain technology and local differential privacy. Llanos et al. [20] examine the challenges of cloud service transparency. The PACE initiative uses Blockchain to protect data. Rahman et al. [40] introduce "DistB-SDCloud," a blockchain-SDN hybrid made to improve cloud computing security.

Prasad et al. [21] focus on wireless network vulnerabilities. They also suggest using an Intrusion Avoidance System (IAS) protocol to secure such networks. Zhang et al. [22] examine cloud-attended e-health system risks. To improve EHR security and integrity, the authors suggest using a blockchain-based system. According to Alzoubi et al. [26], incorporating blockchain technology into Fog computing is proposed as a potential solution for addressing security and privacy concerns associated with this computing paradigm. In their study, Kumar and Nagalakshmi [41] examine the information-focused healthcare model and propose a patient information management system that utilizes blockchain technology. In this study, Rashmi et al. [42] examine the challenges related to scalability and interoperability that emerge when integrating Blockchain with cloud computing. They recommended strategic investment as a means to effectively leverage the advantages offered by this fusion. The study conducted by Li et al. [32] centers around the examination of trust-related concerns within cloud computing. The authors propose the implementation of a decentralized architecture as a means to facilitate distributed trust.

Tehrani et al. [28] examine the concerns around privacy and security in the context of cloud computing. The authors propose that blockchain technology could potentially serve as a solution to

these challenges. In their study, Raju et al. [23] put forth a healthcare privacy paradigm incorporating deep learning techniques to enhance security. Similarly, Yakubu et al. [24] introduce an architecture that preserves privacy and ensures transactional data security within private networks. The architecture proposed by Lou et al. [44] presents a method for enhancing key distribution efficiency through the utilization of Ethereum.

The authors Park et al. [13] propose the utilization of blockchain technology in cloud environments as a means to enhance security. In their study, Darwish et al. [35] propose the use of a hybrid algorithm as a means to augment data integrity and privacy within cloud networks. Qi et al. [19] propose using ring identities and smart contracts to authenticate data and secure user revocation. Alshinwan et al. [43] consider adding cloud and blockchain computing to address security issues. In their paper, Ghorbel et al. [34] propose using BC-ABAC to improve cloud access control for robustness.

Together, the findings highlight the transformative potential of blockchain and cloud computing. They also stress the need for more research to address technology and scalability issues. Table 2 based on the above research and discussion.

The study's strengths lie in its extensive and in-depth review of blockchain technology within the realm of cloud computing. It successfully bridges theoretical concepts with practical applications, providing a holistic view of the field. The detailed analysis of blockchain's evolutionary journey and its potential in enhancing cybersecurity and privacy in cloud environments is noteworthy, shedding light on both current practices and future possibilities. Furthermore, the balanced discussion on the opportunities and challenges presented by blockchain in cloud computing, especially focusing on issues like scalability and energy consumption, adds significant value to the paper.

However, the study also exhibits certain limitations. Firstly, while it excels in theoretical exploration, there is a noticeable gap in the focus on practical implementation. Real-world applications of blockchain in cloud computing scenarios are not extensively covered, which could provide valuable insights for practical adaptation. Secondly, the research predominantly relies on a literature review, and thus, incorporating more case studies or empirical data could greatly enhance the validity and richness of its findings. Lastly, the paper briefly addresses the need for adaptive regulatory frameworks but falls short of delving into specific models or detailed recommendations for such frameworks. These areas, if addressed, could significantly strengthen the impact and applicability of the research in real-world scenarios.

6. CONCLUSIONS

The systematic literature review emphasizes the transformative role of blockchain technology in cloud computing, particularly in enhancing cybersecurity and data privacy. It thoroughly explores blockchain's progression from its beginnings in digital currency to becoming a vital tool for cloud security. The study highlights blockchain's decentralized structure and advanced cryptographic methods as key to solving cloud computing's inherent security challenges. Emphasizing features like transparency, immutability, and consensus algorithms, the review illustrates how blockchain contributes to a more secure, reliable, and privacy-centric cloud infrastructure. The paper also examines blockchain's diverse applications across sectors such as smart contracts, digital currencies, and supply chain management, underscoring its benefits like improved security and data integrity in cloud computing. However, it acknowledges the challenges in blockchain implementation, such as scalability, energy usage, and system complexities, and calls for revising legal frameworks to adapt to its decentralized nature. The review concludes by affirming blockchain's crucial role in the future of digital security and privacy, especially in cloud services, and points to its potential impact across various industries, setting a direction for future research and implementation strategies in this domain. Future research in blockchain for cloud computing should focus on practical implementations through empirical studies and case studies, addressing scalability to develop more suitable blockchain solutions for cloud environments. Energy efficiency is another crucial area, vital for sustainable large-scale applications. Additionally, developing specific regulatory frameworks to support blockchain integration while considering legal and ethical aspects is essential. Expanding the research to examine blockchain's application across various industries will provide a broader understanding of its adaptability. Lastly, exploring advanced cryptographic techniques in blockchain systems will further enhance cloud computing security and privacy, aligning

technological progress with evolving industry requirements and ethical standards.

7. FUNDING

This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT5,874].

8. ACKNOWLEDGMENTS

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT5,874].

9. CONFLICTS OF INTEREST

All authors declare no conflict of interest."

REFERENCES:

[1] Abirami, S. (2019). A complete study on the security aspects of wireless sensor networks. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1 (pp. 223-230). Springer Singapore.

[2] Shahzad, F., Pasha, M., & Ahmad, A. (2017). A survey of active attacks on wireless sensor networks and their countermeasures. Arxiv preprint arxiv:1702.07136.

[3] Arshad, A., Hanapi, Z. M., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in iot-based wireless sensor networks. Peerj Computer Science, 7, e673.

[4] Najmi, K. Y., alzain, M. A., Masud, M., Jhanjhi, N. Z., Al-Amri, J., & Baz, M. (2021). A survey on security threats and countermeasures in iot to achieve users confidentiality and reliability. Materials Today: Proceedings.

[5] Ganesh, D. E. (2022). Analysis of Wireless Sensor Networks Through Secure Routing Protocols Using Directed Diffusion Methods. International Journal of Wireless Network Security, 7(1), 28-35.

[6] Farjamnia, G., Gasimov, Y., & Kazimov, C. (2019). Review of the techniques against the wormhole attacks on wireless sensor networks. Wireless Personal Communications, 105, 1561-1584.

[7] Kardi, A., & Zagrouba, R. (2019). Attacks classification and security mechanisms in Wireless Sensor Networks. Advances in Science, Technology and Engineering Systems Journal, 4(6), 229-243.

[8] Yang, G., Dai, L., Si, G., Wang, S., & Wang, S. (2019). Challenges and security issues in underwater wireless sensor networks. Procedia Computer Science, 147, 210-216.

[9] Islam, M. N. U., Fahmin, A., Hossain, M. S., & Atiquzzaman, M. (2021). Denial-of-service attacks on wireless sensor network and defense techniques. Wireless Personal Communications, 116, 1993-2021.

[10] Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., & Park, Y. (2019). Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. IEEE Access, 8, 3343-3363.

[11] Yousefpoor, M. S., Yousefpoor, E., Barati, H., Barati, A., Movaghar, A., & Hosseinzadeh, M. (2021). Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. Journal of Network and Computer Applications, 190, 103118.

[12] Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IOT: a survey. Wireless Personal Communications, 115, 1667-1693.

[13] Chelli, K. (2015, July). Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the world congress on engineering (Vol. 1, No. 20, pp. 876-3423).

[14] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[15] Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017, July). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In 2017 International Conference on Signal Processing and Communication (ICSPC)(pp.288-293). IEEE.[16] Elsadig, M. A., Altigani, A.& Baraka, M. A. A. (2019). Security issues and challenges on wireless sensor networks. Int. J.Adv. Trends Comput. Sci. Eng, 8, 1551-1559

[17] Keerthika, M., & Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. Global Transitions Proceedings, 2(2), 362-367 \bibitem:Vikhyath, K. B., & Brahmanand, S. H.: Wireless sensor networks security issues and

challenges: A survey. Int. J. Eng. Technol, 7(2), 89-94 (2018)

[18] Inayat, U., Ali, F., Khan, H. M. A., Ali, S. M., Ilyas, K., & Habib, H. (2021). wireless sensor networks: security, threats, and solutions. in 2021 international conference on innovative computing (icic) (pp. 1-6). ieee

[20] Goyal, Gourav & Singh, Yudhvir & Dhwaj, Dheer & Malik, dr. (2022).wireless sensor network: attacks and countermeasures

[21] mahajan, m., reddy, K. T. V., & Rajput, M. (2016). Design and simulation of a blacklisting technique for detection of hello food attack on LEACH protocol. Procedia Computer Science, 79, 675–682

[22] Vasudeva, A., & Sood, M. (2018) . Survey on sybil attack defense mechanisms in wireless ad hoc networks. Journal of Network and Computer Applications, 120, 78–118

[23] Patil, A., & Gaikwad, R. (2015) .Comparative analysis of the prevention techniques of denial of service attacks wireless sensor network. Procedia Computer Science, 48, 387–393

[24] Anand, C., & Gnanamurthy, R. K. (2016).Localized dos attack detection architecture for reliable data transmission over Wireless Sensor Network. Wireless Personal Communications, 90(2), 847–859

[25] ZHENSHAN, Bao, BO, Xue, et WENBO, Zhang. (2013).HT-LEACH: An improved energy efficient algorithm based on LEACH. In : Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on. IEEE, 2013. P. 715-718

[26] Palan, N. G., Barbadekar, B. V., & Patil, S. (2017). Low energy adaptive clustering hierarchy (LEACH) protocol: A retrospective analysis. In 2017 International conference on inventive systems and control (ICISC) (pp. 1-12). IEEE.

[27] Pritchard, S. W., Hancke, G. P., & Abu-Mahfouz, A. M. (2018, June). Cryptography methods for software-defined wireless sensor networks. In 2018 IEEE 27th international symposium on industrial electronics (ISIE) (pp. 1257-1262). IEEE.

[28] Chelli, K. (2015, July). Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the world congress on engineering (Vol. 1, No. 20, pp. 876-3423)

Table 1: Overview of Research Publications with Addressed Issues and Proposed Mitigations.

Authors	Publ.	Addressed issue	Proposed mitigation
Wen et al. [21]	2023	This essay focuses on the security and privacy obstacles that arise in broadening the use of blockchain technology in several areas, encompassing digital money, the Internet of Things and smart grids.	This paper examines privacy preservation and security oversight in the context of blockchain applications while also exploring potential avenues for future research to tackle these obstacles.
Qin et al. [23]	2023	The article discusses COVID-19 patient tracing privacy. Traditional ciphertext policy attribute based encryption (CP-ABE) improves security and access control, but strains resource-limited devices and raises privacy leakage concerns after data decryption. Traditional stored-in-the-cloud data management is equally vulnerable to cyberattacks.	A verified ABE system using blockchain and local differential privacy is proposed. To prevent collusion attacks, this system perturbs original data, outsources decryption and encryption to decrease mobile terminal demand, and executes smart contracts fairly in semi-honest cloud-based servers. It is privacy protective and optimized for data precision, computational overhead, retention, and fairness, making it an affordable and reliable tracing system solution.
Llanos et al. [24]	2023	The article discusses the issue of limited transparency and control within the architecture of cloud-based services, which presents difficulties in ensuring data safety and compliance.	The PACE project is focused on developing a technology that utilizes blockchain to augment privacy and safeguard data. This paper delves into the transdisciplinary obstacles, legal and practical limitations, and the inherent conflict between blockchain technology and GDPR. It offers valuable insights that can inform future collaborations between technology and law in data protection.
Prasad et al. [25]	2023	This article discusses cloud computing security and privacy, specifically wireless and mobile communications network vulnerabilities to malicious attacks.	The study offers an IAS protocol with blockchain technology to improve cloud computing security and privacy. This protocol handles identity verification, decentralized key management, and secure authentication. Data access rate, the communication ratio, end-to-end delay, and energy consumption are simulated to evaluate its effectiveness. The BC-IAS protocol uses blockchain's secure and transparent nature with smart contracts for access management to increase cloud computing security and decrease data breaches.
Raju et al. [27]	2023	This study centres on the issue of privacy problems in the use of clouds within ubiquitous healthcare systems, with a particular emphasis on the challenges associated with secure data sharing and communication.	The authors offer a secure healthcare IoT privacy paradigm using deep learning and secure outsourcing. The model secures cloud data with hybridized encryption "(Optimal Key-based Hybrid Elliptic Curve Cryptography with Fully

			Homomorphic Encryption)" and an optimized deep learning network for encryption, storage, and prediction
Yakubu et al. [28]	2023	The research addresses the confidentiality and safety of transactional data in massive private networks, especially cyber physical systems. The concern is preventing privacy breaches from adversaries via exploitation methods.	A privacy-preserving architecture using digital, and blockchain technology is presented in the paper. This model secures and unalters data in transit, ensuring data provenance throughout node-to-node interactions in huge private networks
Gugueoth et al. [29]	2023	This assessment centers on the significant security and privacy challenges arising in the context of the Internet of Things. It emphasizes the heightened vulnerability to data privacy breaches resulting from the progress made in IoT technology.	Blockchain-based solutions for IoT security, IoT security risks, and integration obstacles are examined in the study. It discusses consensus protocols, security methods, and assessment parameters. The study also addresses outstanding questions and offers additional research.
Cao et al. [22]	2022	This article examines the various obstacles encountered in ensuring security and privacy within smart grid systems, specifically focusing on data gathering and energy trading inside public networks.	This paper examines and compares blockchain based technologies as potential solutions for addressing the difficulties above in smart grid systems. The primary areas of attention include privacy preservation, identity verification, data consolidation, and electricity pricing mechanisms. The report further examines the current obstacles and potential avenues for future research
Zhang et al. [26]	2022	The study discusses cloud assisted e-health system security, where hostile doctors may collude with cloud service providers to mishandle or expose patients' EHRs.	A blockchain-based privacy-preserving e-health system could protect patients' EHRs. This system uses pairing-based encryption to build tamper-proof EHR records integrated with transactions on the blockchain for verifiability and illegal modification protection. The solution also uses blockchain-based smart contracts to protect diagnostic and storage payments. Security analysis and performance assessment show the scheme's efficiency and low computational overhead.
Alzoubi et al. [30]	2022	Fog computing, a Cloud computing extension that boosts IoT device processing capability, has security and privacy issues. Fog computing reduces energy usage and latency but raises security and privacy problems.	The study proposes using Blockchain in Fog computing to address these issues. Fog computing applications benefit from blockchain's security, anonymity, distributed trust management, and stability. The poll explores blockchain's potential to improve Fog computing's security and privacy by enabling distributed and trusted identity management, safe data,

			and reliable reputation and payment systems.
Abualsauod [31]	2022	Research focuses on UAV security and privacy, especially when connected with the IoT. Healthcare and traffic monitoring UAVs struggle to secure and protect their IoT frameworks.	The article recommends a hybrid blockchain strategy for UAV-enabled IoT security and reliability. This solution integrates blockchain-based technology to improve system utility, accuracy, latency, and processing time. This methodology shows improvement and suggests new field research areas.
Tehrani et al. [32].	2022	The study addresses cloud computing privacy and security issues. Cloud computing is becoming more popular for its efficiency and availability, yet centralized systems remain vulnerable and confusing.	This article examines the utilization of blockchain technology inside contemporary cloud storage systems, focusing on its potential to mitigate security and privacy concerns. The authors present a proposition for utilizing blockchain technology to overcome the constraints of conventional cloud computing. They provide a comprehensive analysis of the legal and technological aspects involved in implementing blockchain-based solutions.
Wang et al. [33]	2022	This article addresses the difficulty of safe, private information exchange among competing intelligent factories in the IoT, which is necessary to improve intelligent manufacturing defect prediction models.	The authors suggest a blockchain-based IoT method for safe information sharing. It uses Ethereum clients to establish trusted networks, an "Intelligent Elliptic Curve Digital Signature Algorithm for ownership verification, and Reputation-based Delegated Proof of Stake for security". Both theoretical and simulation investigations show the incentive mechanism to stimulate smart factory information-sharing works.
Ferrag et al. [34]	2021	The present study focuses on the many challenges in implementing security and privacy systems based on blockchain technology for Internet of Things applications. When comparing consensus algorithms, there is A degree of variability in performance parameters such as latency, throughput, and scalability. The necessity for implementing comprehensive security analysis and evaluation procedures is evident.	The proposed mitigation includes comparing and reviewing blockchain security technologies for various IoT applications. Using BAN logic, game theory, and AVISPA for security analysis. Creating explicit rules for creating and testing IoT blockchain security systems.
Velmurugadass et al. [35]	2021	This research examines the growing security threat in healthcare, finance, smart applications, supply chain administration, and IoT. It improves blockchain security in IoT cloud computing.	The study introduces a "Cloud-based Software Defined Network (SDN)" with IoT devices that use the "Elliptic Curve Integrated Encryption Scheme (ECIES)" and SHA-256 for security. The technology monitors data,

			encrypts packets, and stores evidence on blockchain for authorized investigators to identify, gather, analyze, and submit evidence.
Li et al. [36]	2021	The study covers cloud computing security and trust issues. Cloud computing is a centralized trust paradigm, which causes management overhead, network congestion, and single points of failure despite its enlarged service area and economic benefits. Trust ratings' lack of openness and traceability also limits user acceptance.	Blockchain technology is suggested for a decentralized cloud computing distributed trust architecture. Blockchain's credibility, undeniability, and security make it suitable for transparent, traceable transaction data, boosting trust.
Picone et al. [37]	2021	The article explores blockchain's novel IoT security use. It emphasizes IoT security and investigates how blockchain technology may help.	This study introduces a novel authentication mechanism based on blockchain technology to manage cloud insiders. The proposed mechanism offers peer to peer authentication and effectively addresses the challenges posed by insider and outsider threats, boosting cloud environments' overall security
Ghorbel et al. [38]	2021	This article examines the necessity of implementing robust access management protocols in cloud services, emphasizing the shortcomings of conventional access control methods and the frequency of unauthorized access breaches.	"BC-ABAC (Blockchain-based Attribute-Based Access Control)" uses blockchain technology to provide dependable, adaptable, transparent, and fine-grained access control while protecting user identity and accountability. A permission blockchain prototype, scalability testing, and threat model research prove the concept is feasible.
Yang et al. [19]	2020	The article discusses cloud computing security, focusing on centralized access control problems. Hackers and internal cloud management can manipulate and disclose sensitive cloud data due to these vulnerabilities.	The authors propose AuthPrivacyChain, a blockchain-based access control system for cloud privacy. Encrypted and stored in the blockchain, this framework alters access control rights. EOS's AuthPrivacyChain prohibits hackers and administrators from accessing authorized users' data, protecting their privacy.
Darwish et al. [39]	2020	Privacy exposure, data loss, manipulation, and service-level agreement violations are major cloud computing privacy and security issues. Because cloud computing networks are centralized, these issues undermine cloud service reliability and trustworthiness.	A blockchain-based hybrid algorithm addresses these difficulties. Data is encrypted before being transferred to data centers and signed on a decentralized blockchain using this revolutionary technology. It was tested on a virtual cloud that mimicked real cloud infrastructure. Despite increased computing needs owing to blockchain integration, the architecture improved

			data integrity, reliability, and user privacy
Wang et al. [18]	2019	The authors address cloud-based EHR security and privacy issues. The centralized nature of cloud computing threatens EHR data security and patient privacy.	The authors suggest a blockchain-based EHR sharing system for privacy and security. Searchable encryption and conditional proxy re-encryption protect data in this protocol. The consortium blockchain has a proof of authorization consensus mechanism to improve system availability and efficiency
Mohanta et al. [20]	2019	The study examines blockchain implementation challenges, including security and privacy. It seeks to give academic researchers an insightful overview of blockchain technology's prospective uses and security and privacy challenges.	The article suggests a detailed study of Blockchain technology's many uses. This study addresses Blockchain implementation obstacles and security and privacy issues to inform academic research. The attempt to consolidate information in this sector is significant.
Abdulkader et al. [40]	2019	Incorporating Blockchain technology into Internet of Things environments presents significant challenges, mostly from IoT systems' constrained computing, storage, and energy resources. Consequently, conventional blockchain solutions are deemed inadequate for addressing these challenges.	The study proposes a lightweight blockchain-based cybersecurity (LBC) architecture for IoT to eliminate the computational expense of consensus techniques. It uses "Edge Block Managers for local blockchain management and Aggregation Block Managers for public blockchain distribution" to achieve fast throughput, low latency, and protection against conventional threats.
Esposito et al. [41]	2018	Due to real-time access to entire patient medical histories and data management cost benefits, healthcare is shifting data and services to the cloud. They warn that traditional cryptography and access control techniques cannot guarantee privacy and security in this cloud-based environment.	Blockchain technology protects cloud-stored healthcare data, according to the authors. They note that blockchain improves data security and privacy, but using it in healthcare is difficult. The report emphasizes the need for more research to address these difficulties and use blockchain for cloud-based healthcare data security and privacy.
Liang et al. [15]	2017	The study addresses cloud data provenance security. Accountability, forensics, and privacy depend on data provenance, which is information that details object creation and actions of cloud data. Tampering and unauthorized access are major concerns in cloud computing; thus, security is crucial.	The authors present ProvChain, a decentralized blockchain-based cloud data provenance architecture. This solution ensures tamper-proof records, openness in data accountability, and cloud-provenance of data privacy and availability. ProvChain provides a solid, low-overhead solution for cloud storage applications by collecting, storing, and validating provenance data.
Dorri et al. [42]	2017	The article highlights a major IoT security and privacy issue in smart homes. The scattered nature of IoT networks and the resource limits of IoT devices make security and	The authors suggest an IoT-specific lightweight blockchain solution that eliminates the need for Proof of Work and coins to decrease resource requirements. The smart home

		privacy safeguards difficult, especially with standard blockchain systems that need a lot of energy and computational power.	framework they have developed incorporates a powerful "miner" device that accomplish critical security objectives while incurring minimal overhead.
Park et al. [17]	2017	This abstract illustrates blockchain's growing popularity as a secure financial solution for peer authentication, encryption, and hash value production. It also predicts further industry growth and blockchain application expansion beyond IoT.	This article recommends incorporating blockchain computing into cloud computing settings to improve security. It uses blockchain's peer authentication, encryption, and hash value generation to secure cloud computing. A careful examination of blockchain's security properties and how they might be applied to cloud computing could improve IT security.
Rajendran et al. [43]	2020	This paper examines the significant issue of safeguarding data security and preserving user privacy in diverse network technologies, particularly in light of the growing incorporation of the Internet in applications such as cloud computing, and wireless networks. This statement underscores the importance of developing effective strategies to tackle the security and privacy challenges that arise in a dynamic digital environment.	This study suggests the utilization of blockchain technology, characterized by its decentralized nature and immutability, as a viable approach to bolstering network privacy and security. The task at hand entails the examination of contemporary research pertaining to the utilization of blockchain technology in various networks, with the aim of comprehending its efficacy in mitigating security concerns.
Zhang et al. [14]	2023	The paper examines two primary concerns pertaining to the utilization of blockchain technology in mobile cloud computing (MCC) services. The utilization of blockchain technology in MCC applications introduces notable security and privacy risks for users. These risks arise from the inherent features of Blockchain, such as its transparency and immutability, which can potentially compromise the confidentiality and security of users' access behaviors. The utilization of encryption techniques in data management on the Blockchain presents several challenges. Although encryption promotes security and privacy, the management and upgrading of access rights in an encrypted format pose difficulty.	In order to address these concerns, the article presents a solution. The proposed method is a blockchain-based solution that enables users to authenticate themselves across many MCC services using a single credential. Additionally, it provides a hierarchical access control mechanism to effectively manage and regulate different levels of access permissions. Pedersen commitments are employed to obfuscate data on the publicly accessible ledger, so guaranteeing both privacy preservation and the capacity to conduct audits. The approach additionally facilitates the implementation of adaptable and fluid updates in an encrypted format.
Rahman et al. [44]	2023	The abstract emphasizes the difficulty of guaranteeing the preservation of data confidentiality, honesty, and security during the	In order to address the aforementioned security challenges, this study presents "DistB-SDCloud," a novel architectural framework that combines

		process of connecting with online computing platforms. Despite the notable progress made in technologies such as Blockchain (BC) and Software Defined Networking (SDN), there are substantial security issues and concerns, particularly when it comes to the exchange of sensitive information within cloud infrastructure.	Blockchain and SDN. The objective of this architectural design is to augment the security of cloud systems by the use of distributed blockchain techniques, specifically focusing on aspects such as security, confidentiality, privacy, and data integrity. Additionally, the integration of SDN is employed to boost the resilience, stability, and load distribution capabilities of the underlying cloud infrastructure.
Kumaret al. [45]	2023	The article discusses the issue of effectively managing and transmitting health records in the healthcare industry, particularly in light of the transition towards a healthcare model that emphasizes the use of information. The article presents a proposed solution for patient information management, which utilizes blockchain technology.	This solution is referred to as the "Blockchain-based Privacy-Preserving and Robust Healthcare data (BPPRH)" system. The present method facilitates the secure transmission of medical data to patients through the utilization of a cloud infrastructure, which incorporates hypervisors and virtual machines (VMs).
Rashmi et al. [46]	2023	Blockchain-cloud computing research is pioneering and has major ramifications for commercial data management, according to the report. This integration has many benefits but also many significant challenges. Scalability, interoperability, security, regulatory compliance, and handling the technological challenges of mixing Blockchain and cloud-based computing platforms are among these issues.	To capitalize on the potential advantages offered by this amalgamation, which include heightened security, improved efficiency, cost-effectiveness, and the emergence of novel applications such as digital identification and decentralized banking, the scholarly article proposes the necessity of strategic planning and financial investment.
eQi et al. [23]	2023	This study examines the intricate data security issues that emerge while sharing group data in cloud computing systems. This particular aspect draws attention to the challenge of upholding data security in the event of a user's departure from a group, hence requiring the re-signing of the remaining data block signatures.	This study presents an innovative approach that integrates ring signatures with smart contracts to tackle the difficulties above. The proposed methodology entails the utilization of linkable ring signatures as a means to generate novel metadata to ensure integrity. This approach enables anonymous verification while concurrently facilitating secure user revocation. Smart contracts are utilized to mitigate the risk of collusion attacks and oversee the handling of malicious re-signing computations
Alshinwan et al. [47]	2023	The essay highlights a significant obstacle encountered in integrating blockchain technology and cloud-based computing. Blockchain technology, renowned for its utilization in digital currencies, has	The essay posits the integration of cloud-based computing and blockchain computing as a potential resolution to the challenges above. This integration aims to enhance various facets like network control, task planning,

		advantages such as heightened security and confidentiality. However, it encounters a notable challenge in terms of scalability, which restricts its capacity to accommodate a wide range of transactions in large quantities.	accuracy of data, resource management, pricing, equitable payment, and allocation of resources. This paper provides an extensive examination of the amalgamation of cloud-based computing and Blockchain as a Service (BaaS), specifically emphasizing the importance of BaaS platforms in business applications

Table 2: A Comprehensive Analysis of Advantages and Limitations.

Paper	Year	Advantages	Limitations
Zhang et al. [26]	2023	Unified authentication system for MCC using Blockchain.	Challenges with encryption techniques and access rights.
Liang et al. [15]	2017	ProvChain for secure cloud data provenance.	Need for comprehensive security solutions.
Wang et al. [18]	2019	Blockchain-based EHR system for data protection.	Issues with centralized cloud computing security
Rajendran et al. [43]	2020	Blockchain for enhanced internet-based privacy and security.	Addressing dynamic digital environment challenges.
Esposito et al. [41]	2018	Blockchain for cloud-stored healthcare data security.	Difficulty in application within healthcare.
Yang et al. [19]	2020	AuthPrivacyChain for cloud privacy and access control.	Vulnerabilities due to centralized access control.
Mohanta et al. [20]	2019	Detailed study of blockchain applications for security.	Challenges in implementation and security concerns
Wen et al. [21]	2023	Exploration of privacy preservation in blockchain applications.	Security and privacy obstacles in diverse areas.
Cao et al. [22]	2022	Blockchain solutions for smart grid security and privacy.	Obstacles in data gathering and energy trading.
Qin et al.[23]	2023	Blockchain and privacy system for COVID-19 tracing.	Privacy leakage concerns and cyberattack vulnerabilities.
Llanos et al. [24]	2023	PACE project for data protection using Blockchain.	Transparency and control challenges in cloud services
Rahman et al. [44]	2023	"DistB-SDCloud" framework combining Blockchain and SDN.	Security issues in sensitive information exchange
Prasad et al. [25]	2023	IAS protocol for cloud computing security.	Network vulnerabilities to malicious attacks
Zhang et al. [26]	2022	A blockchain system for e-health EHR security.	Security threats from hostile insiders.
Alzoubi et al. [30]	2022	Blockchain for security in Fog computing.	Security and privacy issues in Fog computing
Kumar et al. [45]	2023	BPPRH system for secure health record management.	Managing the transition to an information-focused model.
Rashmi et al. [46]	2023	Strategic planning for blockchain-cloud integration.	Scalability and interoperability issues.
Li et al. [36]	2021	Decentralized trust architecture for cloud computing.	Centralized trust paradigm and management overhead.
Tehrani et al. [32]	2022	Blockchain technology for cloud storage systems security.	Privacy and security issues in cloud computing

Raju et al. [27]	2023	Secure healthcare privacy paradigm with deep learning.	Challenges with secure data sharing in healthcare systems.
Yakubu et al. [28]	2023	Privacy-preserving architecture for transactional data.	Privacy breaches from exploitation methods in networks
Lou et al. [39]	2023	Ethereum framework for key distribution in cloud systems.	Limited transparency and control within cloud architecture.
Park et al. [17]	2017	Blockchain computing for enhanced security in cloud settings.	Growing demand for secure financial solutions.
Darwish et al.[39]	2020	A blockchain-based hybrid algorithm for cloud privacy.	Privacy exposure and data manipulation concerns
Qi et al. [23]	2023	Ring signatures and smart contracts for data integrity.	Data security issues during group data sharing
Alshinwan et al. [47]	2023	Integration of blockchain and cloud computing.	Scalability issue restricting transaction support.
Ghorbel et al. [38]	2021	BC-ABAC for robust cloud service access management.	Shortcomings in conventional access control methods.