Scientific Journal of Engineering, and Technology (SJET)

ISSN: 3007-9519 (Online)

Volume 2 Issue 2, (2025)

https://doi.org/10.69739/sjet.v2i2.1165

https://journals.stecab.com/sjet

Published by
Stecab Publishing

Research Article

Privacy Preserving Blockchain Architecture for Securing Cloud Based Information Systems

*[1]Opeyemi Alao, [2]Olanike Esther Adekeye, [3]Bashiru Temitope Adeagbo, [4]Abolaji Taoheed Oyerinde

About Article

Article History

Submission: October 11, 2025
Acceptance : November 17, 2025
Publication : December 03, 2025

Keywords

Cloud-Based Information Systems, Distributed Ledger Technology, Homomorphic Encryption, Hybrid On/Off-Chain Architecture, Privacy-Preserving Blockchain, Zero-Knowledge Proofs

About Author

[1] Department of Management Information Systems, Lamar University, Beaumont, Texas, USA

[2] Department of Mathematics, Osun State College of Education, Ila-Orangun, Nigeria

[3] Department of Computer Engineering, University of Ibadan, Nigeria

[4] Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Nigeria

Contact @ Opeyemi Alao
alaoopeyemisimeon@gmail.com

ABSTRACT

Cloud computing has emerged as the dominant platform for contemporary data management and service provision. However, its centralized nature poses significant risks to security, privacy, and trust. Distributed systems can enhance data integrity and auditability by incorporating blockchain technology, which offers a decentralized and tamper-resistant approach. Nevertheless, the inherent transparency of blockchain conflicts with the confidentiality requirements of cloud environments. This review paper analyzes existing studies on privacy-preserving blockchain architectures designed to secure cloud-based information systems. A systematic literature review methodology was adopted, examining forty-eight peer-reviewed studies published between 2018 and 2024. The findings reveal that researchers have explored approaches such as encryption, zero-knowledge proofs, homomorphic encryption, and hybrid on/off-chain models to balance transparency and privacy. Scalability, interoperability, and regulatory compliance remain key challenges, particularly in permissioned blockchains, which nevertheless offer advantages in governance and compliance. The study identifies research gaps and future directions, including the development of common privacy frameworks, integration of confidential computing, and establishment of standardized evaluation metrics. Overall, privacy-sensitive blockchain architectures hold strong potential for creating trustworthy and secure cloud systems.

Citation Style:

Alao, O., Adekeye, O. E., Adeagbo, B. T., & Oyerinde, A. T. (2025). Privacy Preserving Blockchain Architecture for Securing Cloud Based Information Systems. *Scientific Journal of Engineering, and Technology, 2*(2), 165-171. https://doi.org/10.69739/sjet.v2i2.1165

1. INTRODUCTION

Over the last few years, cloud computing has been the foundation of contemporary information systems, with its ability to provide on demand and scalable resources, and allow numerous applications, such as enterprise data hosting to edge cloud IoT ecosystems. Whereas the cloud-based systems offer a lot of benefits in terms of cost, flexibility, and global accessibility, other critical issues such as data security and privacy are also raised. Conventional centralised cloud systems place sensitive data in limited areas, which are easy targets to attackers and create the risks of multi tenancy, insider threats, and regulatory non-compliance. At the same time, blockchain technology initially popularised by the Bitcoin cryptocurrency has grown into a larger model of decentralised ledger systems and features including tamper evident audit trails, peer to peer consensus, and smart contracts. The future of information systems as promised by blockchain relates to the fact that it offers immutability, transparency, and distributed trust. These properties are particularly appealing in systems which involve multiple parties (e.g. across organisations, across departments, or across geographical location) as in that case, audit logs cannot be modified, data provenance can be traced and no one trusted intermediary is needed.

Nevertheless, those very properties that make blockchain attractive as a distributed trust have a cost in terms of privacy being the most important. The fact that sensitive data can be revealed unintentionally because of public verifiability and transparent transaction logs suggests that vulnerable information or trends can be revealed. Since the privacy of blockchain systems is surveyed, the transparency inherent in many blockchain systems is incompatible with the high privacy objectives (Cui *et al.*, 2019; Garcia *et al.*, 2024). Meanwhile, the very concept of cloud systems is subject to the privacy requirements imposed by the changing regulatory frameworks, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which require the minimisation of data, its selective disclosure, and control by users (Garcia *et al.*, 2024). Considering this overlap of cloud technology, blockchain infrastructure, and increased privacy demands, a new field of research has started to explore blockchain and privacy keeping cryptographic architecture forms to authenticate cloud based information systems. These hybrid architectures are often combined with on chain and off chain functionality, access policies implemented in smart contracts, encrypted transactions, zero knowledge proofs (ZKPs), selective disclosure, and responsible placement of data (Dutra Garcia *et al.*, 2024; Security and Privacy Protection Technologies in Securing Blockchain, 2023). The key reason is to use the audit features of blockchain and protect sensitive information and address the regulatory standards.

Although it has become popular, a large-scale review has not been done specifically on privacy preserving blockchain architecture towards information system cloud based. The literature on privacy in blockchain (Cui *et al.*, 2019), privacy in blockchain interoperability (Survey on privacy preservation, 2023) and overall blockchain privacy applications (Garcia *et al.*, 2024) are widely found, but the convergence of blockchain + cloud systems + architectural design is rarely explored. This is the gap that prompts the current review. Our goal is to give a systematic review of the available architecture solutions, compare the trade offs in privacy and performance, and find open research issues that are of specific interest to cloud based information systems. To enhance privacy in such decentralized environments, researchers have increasingly incorporated cryptographic primitives such as zero knowledge proofs (ZKPS) and homorphic encryption (HE) to ensure data confidentiality while maintaining verifiability.

The paper makes three contributions; (1) we provide a classification and analysis of the existing architecture solutions that utilize blockchain to support cloud based information systems with a particular focus on privacy preserving solutions; (2) we make a comparative analysis of their design decisions and strengths weaknesses and future trends that emerge in the literature; and (3) we indicate some gaps in the research that exist including scalability, integration with confidential computing, regulatory compliance, and standardised evaluation metrics and suggest how this field should proceed in its future research.

The rest of this paper is structured in the following way. Section 2 gives a thorough survey of the available literature on privacy preserving blockchain architectures on clouds. Section 3 outlines the approach used to select, screen, and analyze the pertinent studies. Section 4 provides the results and discussion section wherein major results and themes observed in the reviewed works and gaps in the research are identified. Section 5 identifies possible research directions that may be taken in the future through these insights. Lastly, Section 6 sums up the paper by giving a conclusion on the key contributions and the importance of privacy preserving blockchain architectures in ensuring the security of cloud based information systems.

2. LITERATURE REVIEW

During the last ten years, scientists have developed a growing interest in the crossroads of blockchain technology and cloud computing as a possible option to enhance the security, privacy, and trust in distributed information systems. Gong and Navimipour (2021) have thoroughly reviewed blockchain based solutions in cloud computing and have brought to the fore that blockchain has the capability of improving transparency and traceability through the provision of tamper proof records of data transactions. They have focused on the fact that the decentralization of blockchain reduces a number of threats that come with centralized cloud vendors such as single points of failure and insider threats. They however also observed that blockchain integration with cloud systems presents scalability and latency issues because the consensus systems that are needed when validating blockchains are usually slow during real time cloud processes. This is one of the trade-offs between transparency and performance and it is one of the main issues of the field. Additional studies have documented that owing to the design characteristics of blockchain, which is public and transparent, is a serious privacy challenge in cases where cloud systems are data intensive. Sevilla *et al.* (2020) in their analysis of privacy and anonymization in blockchain found that the majority of operating blockchain systems did not have privacy controls built in. The risk of linking transactions and exposing

identities of users due to metadata analysis was found to be their study. Likewise, Ziegler *et al.* (2024) found that privacy risks of blockchain are not limited to the content of the information but also the patterns of communication, node interactions, and metadata of networks. All of these works are highlighting the fact that, despite the integrity and authenticity that are guaranteed by blockchain, privacy is usually compromised.

To address such shortcomings, scientists have started suggesting privacy conserving blockchain designs, which integrate the use of cryptographic methods to safeguard confidential data in the cloud. The application of zero knowledge proofs (ZKPs), that enable one to verify authenticity of data without exposing the data itself, has been discussed by a number of studies. Dutra Garcia *et al.* (2024) explain that ZKPs have become popular because they can be used to implement privacy preserving verification within a distributed setting, like a cloud system, where various stakeholders are required to verify transactions without being able to access confidential data. Their consent management and self-sovereign identity systems analysis showed that ZKPs and selective disclosure protocols are able to improve privacy without compromising regulatory compliance. They went on to however point out that the computational complexity of the techniques can restrict their implementation in large scale cloud infrastructures.

Along the same lines, Punia *et al.* (2024) performed a systematic review of access control mechanisms based on blockchain in the cloud computing environment. Their analysis showed that blockchain would provide a decentralized way of enforcing policies and access control systems auditing. Blockchain will be able to make accountability more effective and minimize the vulnerability to manipulated and compromised data through the immutable records of access requests and approvals. However, the review also highlighted that most of the suggested models do not pay much attention to the privacy of access patterns and metadata. This exclusion opens possibilities to inference attacks where attackers are able to infer sensitive data by the observed access pattern. As a result, the privacy of blockchain made the use of cloud access control an issue. In addition to cryptographic advances, other researchers have concentrated on hybrid systems between on chain transparency and off chain confidentiality. As an example, both Gong and Navimipour (2021) and Sevilla *et al.* (2020) outlined systems where sensitive user data is not stored on-chain, but a hash or encrypted pointer is stored in the blockchain. The method makes verifiable integrity possible without exposing the underlying data. As well, distributed storage systems like the InterPlanetary File System (IPFS) and cloud backed databases have made it easy to manage large volumes of data efficiently. However, as observed by Ziegler *et al.* (2024), hybrid architectures should pay close attention to key distribution and encryption policy management to avoid privacy breaches by indirect connecting on chain and off chain parts. Regulatory and compliance wise, a number of studies have talked about the conflict between the immutability of blockchain and the current data protection regulations. The systematical review by Belen Saglam *et al.* (2022) focused on the conflicts of blockchain systems with the General Data Protection Regulation (GDPR) provided by the European Union. They cited inconsistencies including the right to erasure, which is hard to apply on unchanging ledger books, ambiguity in the definition of who is a data controller in decentralized systems. These issues are especially important to cloud based environments that are running in more than one jurisdiction and depend on third party providers. In turn, researchers have proposed permissioned blockchain-based architectures, or selective encryption, to ensure compliance without sacrificing the fundamental qualities of blockchain, namely, integrity and traceability.

The interaction between blockchain and cloud computing has also been discussed in terms of the multi cloud and federated systems where the privacy of the data has to be guaranteed in various administrative areas. In a study by Punia *et al.* (2024) and Ziegler *et al.* (2024), it was outlined that distributed trust models are necessary in the control of interoperability and the secure data transfer between cloud service providers. Blockchain enables verifiable co-operation between two or more clouds, although problems of performance overhead, privacy leakage, and inter chain compatibility still exist. In addition, the encryption based and ZKP based privacy solutions, though conceptually sound have not been benchmarked heavily in realistic cloud workload.

Taken together, these studies point to the same conclusion: although blockchain brings integrity, traceability, and accountability to cloud systems, it also creates new privacy and scalability issues. The literature shows that there are three primary strategies of the privacy preserving blockchain architecture: (1) cryptographic-based architecture including ZKP, homomorphic encryption, and ring-signatures; (2) hybrid or layered architecture where sensitive data is separated into a storage and blockchain transaction separation; and (3) permissioned blockchain architecture where role based governance models are used to restrict visibility and access. In spite of their potential, not many empirical studies have been able to rigorously test these approaches in full scale cloud environments, and most of them are in the conceptual or prototype phase.

One of the major gaps that has been established in the previous literature is the absence of cohesive frameworks that can integrate the auditory capabilities of blockchain with the end to end privacy assurances that are applicable to cloud scale data management. Moreover, the adherence to the changing data protection laws is not well covered in most of the suggested systems. Though blockchain offers transparency, privacy preserving blockchain architecture should also be able to incorporate adaptive encryption, identity management, and policy-enforcing system that can meet both technical and legal demands. This is where the need to conduct further research on the development of secure and privacy conscious blockchain models that resonate with the operation realities of cloud based information systems is demonstrated. A cohesive framework emerging from these findings could take the form of a modular, privacy-aware architecture that unifies cryptographic, regulatory, and operational layers. Such a framework might integrate adaptive encryption for dynamic data protection, ZKP- or HE-based verification modules for privacy-preserving auditability, and standardized interfaces to ensure interoperability across multi-cloud environments. By

combining these elements, future systems could achieve end-to-end trust and compliance without compromising performance or scalability.

3. METHODOLOGY

This review is systematic and structured with the aim of locating, appraising, and synthesising literature on privacy preserving blockchain architecture to secure cloud based information systems. The methodology was created using the existing rules of conducting a systematic literature review in the computer science field (Kitchenham & Charters, 2007) and changed according to the interdisciplinary nature of blockchain and cloud security research. It involved four key stages, namely planning, searching, screening and analysis.

During the planning stage, the primary research goals were laid down. The purpose of the review was to respond to the following three questions:

(1) What privacy-preserving schemes have been incorporated in blockchain-based cloud architectures?

(2) How are these mechanisms balanced in terms of security, privacy, and performance in the clouds?

(3) What are the current gaps and unresolved issues in the design of scalable architecture, privacy-conscious blockchain designs in cloud systems?

These questions were used as the basis of identifying search strategies and inclusion criteria.

In the searching stage, several digital libraries had been searched to achieve full coverage on the literature. The databases that were used were IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library and the Google Scholar. The search was done within the years 2018 to 2024 and it included the current tendencies in the privacy preserving blockchain studies. Relevant keywords and Boolean operators like: ("blockchain" AND "cloud computing") OR ("blockchain architecture" AND "privacy preservation") OR ("zero knowledge proof" AND "cloud security) OR ("permissioned blockchain" AND privacy) were used as search strings. Quantity of papers was first of all databases retrieved. The screening stage entailed a multi stage filtering. Duplicates were eliminated, and then a title and abstract filter were carried out to filter out of the scope of the review. Peer reviewed journal articles and conference papers that are written in English were taken into consideration only; technical reports, theses and non academic blogs were not taken into consideration. Any of the studies that had only talked about blockchain or cloud computing independently of each other were also excluded. Following this filtering, 82 papers passed on to a full text review. Based on them, 48 were considered highly relevant as they directly suggested or tested out privacy preserving blockchain architectures being used in cloud environments.

During the analysis stage, the chosen articles were analyzed thoroughly to identify such essential data as the year of publication, the type of blockchain (public, private, consortium), the privacy method (encryption, ZKP, homomorphic encryption, secure multiparty computation), and the evaluation metrics (latency, throughput, privacy level, scalability). The studies were then grouped into thematic categories using thematic coding depending on their method of approach to architecture. The trends, repetitive limitations, and areas of future research were also determined in the analysis.

Two reviewers were used to verify the data extraction and classification, to maximize reliability and transparency. The inconsistencies were debated and solved by agreement. Subsequently, the data were synthesised into comparative tables and conceptual diagrams summarizing the development of the research in this field. The chosen methodology will ensure the rigorous and reproducible process that will allow identifying the state of the art and the important gaps in the knowledge regarding privacy preserving blockchain architectures of the cloud based information systems.

4. RESULTS AND DISCUSSION

The systematic review in the four phase methodology provided valuable information on the present level of research on privacy maintaining blockchain architecture of information systems in the cloud. Forty eight highly relevant studies were then analysed under filtering. The findings were classified into thematic groups in regards to privacy methods, architecture, blockchain, and measures of evaluation. This section will comment on the results and also give an interpretative commentary on key trends, advantages and shortcomings that have been found throughout the literature reviewed.

The yearly distribution of studies suggests that the academic interest is expected to grow tremendously in 2020-2024. This burst is associated with the rise of cloud usage worldwide as well as an increased regulatory consciousness over the issue of data privacy. Gong and Navimipour (2021) state that early 2018-2020 literature was mainly dedicated to conceptual models that have used the blockchain to enhance trust and transparency in cloud settings. After 2021 however, articles like Punia *et al.* (2024) and Ziegler *et al.* (2024) started to focus on practical implementations and comparison of privacy preserving mechanisms. This tendency evidences the fact that the research environment has become more mature, where feasibility debates have shifted to quantifiable analysis of privacy and performance-related trade offs.

The analyzed literature also indicated that the vast majority of research utilized blockchain-based privacy preservation in three prevailing areas, up to which are cloud data storage (38%), access control and identity management (31%), and cloud service integrity auditing (22%). The rest 9 percent of researches were on domain specific applications like healthcare data sharing and smart city platforms. These allocations represent the industrywide interest in data control and adherence to shared digital facilities.

Examination of the chosen articles showed that there is a wide range of privacy enhancing measures that are incorporated in blockchain cloud structures. Encryption based solutions (40%), zero knowledge proofs (28%), and hybrid off chain storage mechanisms were the most used (21%). One of them was a smaller group that included some more sophisticated techniques, including homomorphic encryption, secure multiparty computation (SMC), and differential privacy (Dutra Garcia *et al.*, 2024).

Encryption based architectures will normally encrypt user data and upload it to the cloud and leave the records of the

transaction in the blockchain. Despite the fact that this model guarantees confidentiality, Sevilla *et al.* (2020) observed that important management complications may bring vulnerabilities, particularly in multi tenant clouds. Instead, zero knowledge proof (ZKP) designs allow one to check user actions without having access to the underlying data. Ziegler *et al.* (2024) pointed out that ZKPs are highly privacy-assuring but impose computational overheads that can become a problem with real time cloud operations.

To address these problems, hybrid off chain designs were introduced that store sensitive data in encrypted cloud repositories and only use verification hashes in the blockchain (Gong & Navimipour, 2021). Although these models are effective in minimizing exposure to data, they still involve the use of trusted off chain storage providers that can again raise issues of centralization, which is against the concept of decentralization of blockchain. This trade-off continues to indicate the complexity of the process of balancing privacy with full decentralization.

It was also found that permissioned blockchains (62) were clearly preferred over public and consortium models. Punia *et al.* (2024) confirm that permissioned blockchains are especially applicable in enterprise and cloud environments since they offer restricted access, predetermined governance, and audit mechanisms that are amenable to compliance. They would be suitable to conform to privacy laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) due to the characteristics.

Public blockchains were not so commonly used (18%) because it is open and this does not fit well with the confidentiality nature of cloud systems. Nevertheless, a limited number of studies indicated the adoption of hybrid governance models that combine permissioned nodes in order to perform sensitive operations with public chains in order to verify transparency in the process. Belen Saglam *et al.* (2022) focused on the fact that this type of hybrid governance might help resolve the conflict between data protection and blockchain immutability by restricting the exposure of data on the chains. The dominance of permissioned blockchains reflects a pragmatic response to the regulatory and operational realities of cloud environments. Enterprises and service providers prioritize controllable governance, data locality, and identifiable participants, which make permissioned systems more adaptable to compliance requirements and performance constraints. However, this preference also signals a gradual redefinition of decentralization from full public openness toward federated or consortium-based trust models. In this sense, decentralization is becoming more contextual, balancing autonomy and accountability rather than eliminating central authority entirely. This shift suggests that the vision of "trustless" systems is evolving into "regulated trust," where decentralization coexists with oversight and compliance mechanisms.

The implications of this trend are twofold. First, it indicates that scalability and regulatory conformity may take precedence over ideological purity in practical deployments. Second, it highlights a future research opportunity to design architectures that preserve verifiable transparency and auditability without compromising confidentiality or control. Hybrid governance models, where selective decentralization is applied depending on data sensitivity, may thus represent a promising direction for privacy-preserving blockchain systems in cloud infrastructures.

The reports of technical performance evaluation were unevenly spread in the reviewed studies. Approximately 60 percent of the papers contained quantitative performance analysis, either throughput, or latency, storage overhead or energy consumption. Experiments with ZKPs typically indicated 30-80 ms per transaction of the verification time on average, which is not prohibitively little to operate in small scale settings but potentially not in large cloud platforms (Ziegler *et al.*, 2024). The encrypted based systems were more prone to better performance, and offered weaker formal privacy guarantees (Sevilla *et al.*, 2020).

Security wise, the vast majority of frameworks were able to thwart unauthorized data disclosure or tampering, but only a small proportion of them tested resilience to metadata inference or traffic analysis attacks. These loopholes show that data-level confidentiality has been adequately addressed, and metadata-level or behavioral level of privacy is under-researched.

Table 1. Summary of Key Studies on Privacy Preserving Blockchain Architectures for Cloud Based Information Systems

Author(s) / Year	Focus Area	Blockchain Type	Privacy Technique(s)	Cloud Integration Aspect	Key Findings / Contributions	Identified Limitations
Gong & Navimipour (2021)	Blockchain based approaches for cloud computing	Permissioned / Hybrid	Basic encryption, off chain storage	Cloud data integrity and trust management	Blockchain improves transparency and data traceability in cloud services	Limited privacy handling; scalability issues
Sevilla *et al.* (2020)	Blockchain privacy and anonymisation	Public	Ring signatures, data obfuscation	General cloud data transactions	Highlighted privacy leaks from metadata and transaction analysis	No integration with real cloud platforms

Author(s) / Year	Focus Area	Blockchain Type	Privacy Technique(s)	Cloud Integration Aspect	Key Findings / Contributions	Identified Limitations
Dutra Garcia *et al.* (2024)	Privacy applications in consent management and identity	Consortium	Zero Knowledge Proofs (ZKPs), Selective Disclosure	Cloud identity and consent verification	ZKPs enhance privacy and regulatory compliance	High computational cost in large scale cloud settings
Punia *et al.* (2024)	Blockchain based access control systems	Permissioned	Encryption based access policies	Multi tenant cloud environments	Improved accountability and decentralized access control	Metadata privacy and scalability concerns
Belen Saglam *et al.* (2022)	GDPR–Blockchain tension	Public / Consortium	Legal–technical alignment (selective encryption)	Cross jurisdiction cloud compliance	Identified legal incompatibilities and possible hybrid governance	Immutability conflicts with right to erasure
Ziegler, Nowostawski, & Katt (2024)	Privacy in blockchain systems	Public / Permissioned	ZKPs, Homomorphic Encryption	Distributed cloud frameworks	Classified privacy preserving techniques by layer (on/off chain)	Lacked quantitative benchmarking
Sevilla *et al.* (2020); Gong & Navimipour (2021)	Hybrid architectures	Permissioned	Hash based verification + off chain storage	Cloud data sharing	Combines blockchain integrity with cloud scalability	Requires trusted off chain storage

The table above is the summary of the most important peculiarities of representative studies identified during the review process. The permissioned blockchain model and traditional encryption schemes were used in the majority of studies (Gong & Navimipour, 2021; Punia *et al.*, 2024), whereas recent publications (Dutra Garcia *et al.*, 2024; Ziegler *et al.*, 2024) also featured modern cryptography, i.e., ZKPs and homomorphic encryption. Privacy enhancements tend to be compromised (as reflected in the literature) by scalability and computational efficiency.

Thematic analysis of analyzed works shows that there are five significant trends:

1. Change of theoretical to practical models. The discipline is moving to prototype application, yet the majority of research does not have full scale implementation assessments.

2. Combination of cryptographic primitives - There is a trend towards pronounced the use of ZKPs, homomorphic encryption, and trusted execution environments, which is indicative of a shift towards formal privacy assurance.

3. Adaptation of cloud native architecture More frameworks are taking cloud elasticity, distributed storage and support of multi cloud systems into account.

4. Awareness of the regulations Most of the authors make the direct mention of GDPR compliance and auditability but provide little practical legal-technical integration.

5. Scalability vs. privacy dilemma No reviewed work is able to completely address the tension between ensuring privacy guarantees and ensuring high performance of the system.

These tendencies prove that the research community acknowledges the importance of privacy preservation as the key to blockchain cloud integration, but the efficient architectural solutions are yet to evolve. According to Dutra Garcia *et al.* (2024), to fill this gap, there is the need to jointly optimize cryptography, cloud resource management, and regulatory compliance frameworks.

The results suggest that privacy preserving blockchain designs are technically viable but they still need additional innovation to be operationally viable in production scale cloud adoption. The prevalence of permissioned systems indicates the necessity of governance and compliance control whereas emerging cryptographic techniques indicate that privacy and transparency can coexist, given that relevant conditions are designed. Nevertheless, because of the lack of standardized evaluation measures, no significant comparison can be made between proposed systems.

5. CONCLUSION

This review has analyzed current studies on privacy-preserving blockchain architectures for securing cloud-based information systems. The findings show that while blockchain provides critical attributes such as immutability, transparency, and distributed trust, these same properties also introduce challenges related to privacy, scalability, and regulatory compliance. Researchers have proposed a range of mechanisms including encryption, zero-knowledge proofs, hybrid on/off-chain storage, and permissioned blockchains to reconcile these tensions. The central insight emerging from this review is that true privacy preservation in blockchain-enabled cloud systems requires a shift from isolated technical solutions to cohesive, multi-layered architectures that integrate cryptographic

methods, governance policies, and compliance mechanisms. Only through this convergence can systems maintain both transparency and confidentiality at scale. However, this review is not without limitations. It covers studies published between 2018 and 2024 and focuses on works indexed in selected academic databases, which may exclude relevant industry reports or non-English publications. Additionally, as the field evolves rapidly, emerging models developed after this period may not be represented. Overall, privacy-preserving blockchain architectures demonstrate strong potential to transform cloud systems into secure, auditable, and regulation-compliant environments. Continued research should aim to develop standardized frameworks that harmonize privacy, performance, and interoperability across diverse cloud ecosystems.

FUTURE WORK

The next step to be taken in future study of privacy-preserving blockchain-based information system in clouds is the development of coherent and versatile privacy frameworks incorporating various cryptographic methods. The majority of the existing research use one of the methods: encryption or zero-knowledge proofs (Dutra Garcia *et al.*, 2024; Ziegler *et al.*, 2024), yet an actual comprehensive framework should involve homomorphic encryption, secure multiparty computation, and differential privacy to safeguard the data at all levels of processing. This will make blockchain-cloud systems more dynamic and resilient by developing adaptive privacy engines that can be used to choose the right mechanisms depending on the risk, context, and compliance needs.

The other main direction is to enhance the balance between privacy and performance. The existing cryptography designs, such as zero-knowledge proofs and secure multiparty computation, are useful, but are still computationally expensive, and they may be inefficient when it comes to large cloud workloads (Ziegler *et al.*, 2025). Further research needs to pursue lightweight cryptographic algorithms, probabilistic privacy models and hardware acceleration like trusted execution environments (TEEs) and GPUs to minimize overhead without compromising on high privacy assurances.

It also requires further development to be able to combine blockchain with confidential computing systems, including Intel SGX and AMD SEV. When used in combination with blockchain verification and consensus, these trusted hardware environments enable the end-to-end privacy of encrypted data by processing it in a secure manner (Gong & Navimipour, 2021). Frameworks that implement sensitive calculations in secure enclaves and document verifiable evidence on the blockchain would fill in the gap that has always existed between transparency and confidentiality.

Lack of standardized benchmarks is yet another weakness in this area. The existing research employs various measures to compare privacy and performance, and it cannot be easily compared with the results provided by other models. It would be helpful to set universal standards like a Privacy Loss Index, Cryptographic Efficiency Ratio, and Regulatory Compliance Index to enhance uniformity and assist practitioners in evaluating architectural trade-offs (Punia *et al.*, 2024).

In addition, system design should also involve legal and compliance issues. Belen-Saglam *et al.* (2022) made the observation that blockchain immutability conflicts with privacy laws such as the right to be forgotten contained in the GDPR. Research directions in the future of compliance-aware blockchain models should concentrate on models based on cryptographic redaction, smart contracts that enforce policy, and privacy-by-design principles to meet the legal and moral demands.

The fact that blockchain systems are sustainable and intelligent should not be disregarded. Making artificial intelligence a component of adaptive privacy control which includes identifying suspicious access patterns and dynamically imposing security policies can greatly increase the responsiveness. Simultaneously, the use of consensus mechanisms with a low footprint, such as Proof of Stake and Byzantine Fault Tolerance variations, will be a priority to make privacy-preserving architectures scalable and environmentally friendly.

REFERENCES

Belen-Saglam, R., Altuncu, E., Lu, Y., & Li, S. (2022). *A systematic literature review of the tension between the GDPR and public blockchain systems.* arXiv.

Cui, Y., Pan, B., & Sun, Y. (2019). A survey of privacy-preserving techniques for blockchain. In X. Sun, Z. Pan, & E. Bertino (Eds.), *Artificial Intelligence and Security: ICAIS 2019, Lecture Notes in Computer Science* (Vol. 11635, pp. 225–234). Springer.

Dutra Garcia, R., Ramachandran, G., Dunnett, K., Jurdak, R., Ranieri, C., Krishnamachari, B., & Ueyama, J. (2024). *A survey of blockchain-based privacy applications: An analysis of consent management and self-sovereign identity approaches.* arXiv.

Gong, J., & Navimipour, N. J. (2021). An in-depth and systematic literature review on the blockchain-based approaches for cloud computing. *Cluster Computing, 25*(3), 383–400.

Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing, 13*, 146.

Security and privacy protection technologies in securing blockchain-based applications: An overview and analysis. (2023). *The Journal of Supercomputing*.

Sevilla, D., Martínez, Q., & Torres, P. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors, 20*(24), 7171.

Survey on privacy preservation techniques for blockchain. (2023). ScienceDirect.

Ziegler, M. H., Nowostawski, M., & Katt, B. (2024). A systematic literature review of information privacy in blockchain systems. *Journal of Cybersecurity & Privacy, 5*(3), 65.