Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/145/2025.21867

Comparative Analysis of the Centralized and Decentralized Architecture of Cloud Computing in terms of Privacy Security

Yilin Chen

Beijing-Dublin International College, Beijing University of Technology, Beijing, China
1964782002@qq.com

Abstract: In an era of rapid technological evolution, cloud computing has become indispensable across various industries due to its cost-efficiency, scalability, and accessibility. Yet, privacy and security concerns persist, as sensitive data can be susceptible to breaches and unauthorized access. At present, the two mainstream cloud computing architectures are centralized architecture and decentralized architecture. Both have advantages and disadvantages in terms of confidentiality, integrity and data availability. This paper employs a comparative analysis of these two architectures, synthesizing insights from recent studies and emphasizing the potential of emerging technologies like blockchain to strengthen privacy protection. By examining both architectures through a high-level lens, this study explores how decentralization, supported by distributed consensus mechanisms, can address vulnerabilities and enhance trust among stakeholders. It can be concluded that a decentralized approach, when underpinned by robust cryptographic methods, offers superior safeguards against evolving threats.

Keywords: centralized, decentralized, privacy, cloud computing

1. Introduction

Cloud computing continues to revolutionize modern data management, with its adoption across various sectors steadily rising [1]. However, concerns remain regarding the protection of sensitive information, as evidenced by reports indicating that 57% of companies face security issues when using cloud services [2]. Although considerable research has explored privacy protection in cloud environments, limited studies offer a broad, comparative perspective that includes emergent technologies such as blockchain. To address this gap, this paper investigates two prominent cloud computing architectures—centralized and decentralized—and evaluates their ability to safeguard privacy through three critical dimensions: confidentiality, integrity, and data availability. This study employs a comparative analysis, synthesizing insights from existing literature and examining how each architecture performs against evolving threats. The first section of the paper outlines the fundamental concepts and technical distinctions between centralized and decentralized cloud computing. Subsequently, the second section delves into a detailed evaluation of both architectures, considering state-of-the-art privacy-enhancing mechanisms and the role of blockchain. By clarifying the strengths and limitations of each model, this research contributes to a more nuanced understanding of privacy protection in cloud environments. Ultimately, the findings aim to guide practitioners, policymakers, and academics toward more secure, reliable, and future-proof cloud computing solutions.

DOI: 10.54254/2755-2721/145/2025.21867

2. Basic concept

Centralized cloud computing is the earliest and probably the most mature cloud computing architecture. In this architecture, all data processing and storage tasks are performed within the centralized data center [3]. Its unified and centralized structure design makes it relatively easy to manage and supervise which could help maintain data integrity. This architectural feature also facilitates the implementation of various noncryptographic and cryptographic security technologies that can enhance confidentiality, including data anonymization [4] steganography [1], Public-key encryption [5], and so on. However, storing and processing data from multiple users or organizations on the same physical servers or storage devices, even within separate partitions or virtualized environments designed to maintain isolation and security, can present certain challenges [6] . The most significant problem with high centralization is that if the core node fails, it will bring relatively serious losses and even the whole system may collapse [7]. This problem has potentially negative effects on confidentiality, integrity, and availability.

In contrast, decentralized cloud computing distributes computing resources across various data centers, edge devices, and even individual computers. This structure results in lower latency and greater expandability, contributing to its widespread adoption today [8]. A more decentralized structure gives it more robustness when facing the risks of single points of failure. This shift from a single point of control to a distributed network introduces greater confidentiality and availability when part of the system is failed. Owing to its decentralized architecture, decentralized cloud computing can mitigate risks originating from within the cloud service provider (CSP) to some extent. Managers within the CSP may illicitly access, leak, or modify data for various purposes. Since the data is distributed across multiple nodes or CSPs, it becomes significantly more challenging to obtain valuable or meaningful information. Although it may have several advantages, it is not perfect. The distinct architecture of decentralized cloud computing may present challenges in the implementation of traditional security technologies, particularly cryptographic techniques that were originally designed for centralized cloud environments. Furthermore, to some extent, the decentralized structure can negatively impact data integrity due to its scattered layout and inherent non-uniformity.

3. Comparative analysis

In evaluating privacy protection within cloud computing, this paper adopts three fundamental criteria—confidentiality, integrity, and data availability—to provide a comprehensive assessment that aligns with established security frameworks [1, 6]. Confidentiality ensures that only authorized entities can access sensitive data, thus protecting it from unauthorized disclosure [1]. Integrity pertains to the protection of data against corruption and unauthorized modifications, thereby upholding trust in the system's outputs. [6]. Data availability ensures that information and services remain accessible even amidst system failures or cyberattacks, a critical aspect in both centralized and decentralized architectures [9].

3.1. Confidentiality

Both solutions have their advantages and disadvantages. For confidentiality, noncryptographic techniques like data anonymization and steganography can be employed in both centralized and decentralized cloud computing, but there are some differences. For centralized cloud computing, a trusted cloud service provider (CSP) is required because the entire anonymization process is carried out by a single CSP. In contrast, the security of decentralized architecture may be improved to a certain extent because the process involves multiple CSPs. Data splitting enhances the security of sensitive data by partitioning it into distinct segments and distributing these segments randomly across various cloud repositories [10]. Data splitting ensures that even if an unauthorized entity

DOI: 10.54254/2755-2721/145/2025.21867

accesses a single fragment, the individual's identity remains concealed [10]. The essence of data splitting is to store data in separate blocks. In centralized cloud computing, CSPs implement isolation strategies for virtual machines, but attacks cannot be fully avoided, and virtual machine migration can alter the security domain [6]. Conversely, decentralized architecture, inherently segmented at the physical level, offers greater advantages in privacy security.

When shifting the focus to cryptographic techniques, data is converted into ciphertext through a key and associated algorithms, making it one of the most robust ways to assure confidentiality [1]. Techniques such as Homomorphic Encryption and Symmetric Key Encryption can be employed in both centralized and decentralized architectures, offering essential security advantages while introducing additional computational overhead [1]. In decentralized deployments, this overhead-encompassing heightened energy use, service latency, and operational complexity—can be especially significant, even though it may distribute trust more effectively among the network's nodes [6]. Emerging technologies such as blockchain can further reinforce confidentiality by leveraging distributed ledger mechanisms, where any data modification requires consensus across multiple nodes, thereby reducing the risk of unilateral compromise [9, 11]. However, adopting blockchain-based solutions also elevates resource demands, as consensus protocols and cryptographic validation introduce additional processing requirements. Consequently, while decentralized systems can inherently mitigate single points of failure, they must also address the elevated costs and technical challenges inherent in advanced cryptographic and distributed ledger strategies.

3.2. Integrity

Another crucial aspect of privacy security to consider is integrity, which pertains to the accuracy, consistency, and reliability of data throughout its lifecycle. In essence, it ensures that data remains unchanged and trustworthy from the point of creation or reception through to its use or processing. Cryptographic techniques such as Identity-based encryption [12], Public-key encryption [5], Attribute-based encryption [13], and Signcryption [14] enhance data integrity by facilitating secure communication and access control. Access control is a security measure that governs who can access or utilize resources, thereby ensuring that only authorized users can view or interact with specific data or systems. They ensure controlled access, authentication, and validation, which is crucial for maintaining data integrity in digital environments. These techniques can be both implemented in centralized and decentralized cloud computing. More broadly, ensuring data integrity in decentralized cloud computing is more challenging due to its complex architecture and increased number of nodes compared to centralized cloud computing. The greater complexity and higher number of nodes complicate management tasks such as access control [7]. Additionally, assessing privacy security requires examining availability, which ensures data is accessible and ready for users or applications when needed. Decentralized structures distribute data and computing resources across a network of decentralized nodes, offering redundancy and resilience, even in the face of network failures or attacks, but requiring solutions for the complexity of ensuring data consistency and integrity among distributed nodes.

However, decentralized cloud computing has shown significant improvements in data integrity with the advancement of digital technologies. Blockchain technology has played a pivotal role in enhancing privacy and security within decentralized cloud environments. As an encrypted, distributed, anonymous ledger system, blockchain establishes a trusted interaction method among untrusted computing nodes, making it well-suited for the distributed structure of edge computing. This technology eliminates the need for centralized management nodes by supporting data integrity and security through encryption and consistency mechanisms such as proof of work [11].

For instance, blockchain-based zero-knowledge verification technology significantly enhances privacy security in decentralized cloud computing by allowing one party to prove the validity of a

DOI: 10.54254/2755-2721/145/2025.21867

statement without disclosing any underlying sensitive data. In access control scenarios, such mechanisms enable users to authenticate themselves without revealing personal details, thereby reducing the risk of data exposure [9]. Similarly, blockchain-based ring signature technology further strengthens data integrity and privacy by allowing a user to sign on behalf of a group, effectively concealing the signer's identity among multiple potential signers. This approach is particularly useful for maintaining tamper-proof records and preventing unauthorized access [9]. Moreover, recent research has demonstrated how the integration of advanced cryptographic techniques with blockchain can provide an additional layer of security in decentralized cloud environments. As an illustration, real-world applications in cloud-assisted IoT systems have successfully combined attribute-based encryption with blockchain technology to enhance data protection and accountability among distributed nodes [15]. In the BC-SABE scheme proposed in this paper, IoT devices generate a large amount of data that needs to be stored in the cloud. By using blockchain-aided searchable attribute-based encryption, both data confidentiality and fine-grained access control are achieved simultaneously. The blockchain replaces the traditional centralized server by managing threshold parameter generation, key management, and user revocation, thereby not only ensuring data security but also improving the efficiency of decryption and token generation.

Furthermore, empirical investigations into these advanced cryptographic approaches have highlighted their potential to address specific challenges inherent in decentralized cloud environments. By employing zero-knowledge proofs and ring signatures in practical settings, researchers have illustrated that these techniques not only uphold rigorous privacy standards but also facilitate secure, decentralized interactions among edge devices. Such implementations offer promising avenues for improving security frameworks and operational efficiency, thereby paving the way for more robust decentralized cloud systems [1].

3.3. Data availability

In terms of data availability, centralized cloud computing architectures often rely on robust data center infrastructures and replication strategies to minimize downtime, yet they remain vulnerable to single points of failure [3, 6]. This centralized approach can lead to data silos and pose privacy concerns, as all data is stored in a single location, making it a prime target for cyberattacks. By contrast, decentralized systems distribute data and computational tasks across multiple nodes, reducing the likelihood that a single outage or targeted attack will compromise overall availability [8]. This distribution enhances resilience and fault tolerance, as the failure of one node does not necessarily impact the entire system. However, managing access control and ensuring consistency across these distributed nodes introduces greater complexity [7] Moreover, the integration of blockchain technology has been proposed to augment availability, as distributed ledger frameworks are capable of maintaining real-time synchronization and validation across nodes [1, 9]. Blockchain's inherent transparency and immutability can enhance data integrity and security. However, the transparency of blockchain raises privacy issues, particularly when transactions need to be linked with personal information. Consequently, while centralized approaches benefit from established infrastructure and simplified oversight, decentralized architectures—and particularly those leveraging blockchain—can offer higher redundancy and reliability against outages and attacks, albeit at the cost of increased operational complexity and coordination challenges [1].

4. Conclusion

Decentralized cloud computing is similar to centralized computing in terms of confidentiality as a whole, but it has more advantages in the implementation of individual-specific technologies and has certain prevention capabilities for internal security risks of CSP. In terms of data integrity, centralized

DOI: 10.54254/2755-2721/145/2025.21867

cloud computing benefits from more centralized management, but decentralized cloud computing has also greatly improved in this respect due to the introduction of new technologies such as blockchain. Finally, in terms of data availability, decentralized cloud computing may have some advantages over centralized cloud computing. In general, with the development of technology such as blockchain and the need for low latency, decentralized cloud computing is a more appropriate choice to ensure privacy security.

Nevertheless, this analysis has its limitations. The current study primarily offers a high-level comparison of centralized and decentralized cloud computing, focusing on privacy protection measures across confidentiality, integrity, and data availability. However, it does not delve into detailed technical implementations or provide quantitative benchmarks. Future research could address these gaps by conducting large-scale empirical assessments, developing standardized metrics for side-by-side comparisons, and exploring performance trade-offs in real-world environments. Additionally, in-depth investigations into specific cryptographic protocols or anonymization frameworks could yield a deeper understanding of their practical effectiveness and overhead. Incorporating emerging paradigms such as edge-cloud orchestration might highlight new ways to manage latency and privacy demands concurrently. Long-term research should focus on creating integrated security models that harness cutting-edge distributed ledger technologies—like blockchain—while also advancing lightweight cryptographic approaches to ensure both robust privacy protections and operational efficiency in decentralized environments.

References

[1] *Hassan, J., Shehzad, D., Habib, U., Aftab, M. U., Ahmad, M., Kuleev, R., & Mazzara, M. (2022). The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges—A Systematic Literature Review (SLR). Computational Intelligence and Neuroscience, 2022, 8303504. doi: 10.1155/2022/830350.*

[2] *Alam, T. (2020). Cloud computing and its role in the information technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), pp.108–115. doi:10.34306/itsdi.v1i2.103.*

[3] *Ren, J., Zhang, D., He, S., Zhang, Y., & Li, T. (2019). A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet. ACM Computing Surveys, 52(6), 125, pp.1–36. DOI: 10.1145/336203.*

[4] *Prasser, F., Eicher, J., Spengler, H., Bild, R., & Kuhn, K. A. (2020). Flexible data anonymization using ARX—Current status and challenges ahead. Software: Practice and Experience. DOI: 10.1002/spe.2812.*

[5] *Yu, Z., Gao, C. Z., Jing, Z., Gupta, B. B., & Cai, Q. (2018). A practical public key encryption scheme based on learning parity with noise. IEEE Access, 6. https://doi.org/10.1109/access.2018.2840119.31918.*

[6] *Sun, Y., Zhang, J., Xiong, Y. and Zhu, G. (2014) 'Data security and privacy in cloud computing', International Journal of Distributed Sensor Networks, 2014, available: http://dx.doi.org.ucd.idm.oclc.org/10.1155/2014/19090.*

[7] *Almutairi, S., Alghanmi, N., & Monowar, M. M. (2021) Survey of Centralized and Decentralized Access Control Models in Cloud Computing. International Journal of Advanced Computer Science and Applications, 12(2). Available at: DOI:10.14569/IJACSA.2021.012024.*

[8] *Westerlund, M., & Kratzke, N. (2018). Towards Distributed Clouds: A Review About the Evolution of Centralized Cloud Computing, Distributed Ledger Technologies, and A Foresight on Unifying Opportunities and Security Implications. 14.In 2018 International Conference on High Performance Computing & Simulation (HPCS) (pp.655-663). Orleans, France. doi:10.1109/HPCS.2018.00108.*

[9] *Wang, D., Zhao, J., and Wang, Y. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. IEEE Access, 8, pp.108766-108781. doi: 10.1109/ACCESS.2020.2994294. https://ieeexplore.ieee.org/abstract/document/9093015.*

[10] *Steyerberg, E. W. (2018). Validation in prediction research: the waste by data splitting. Journal of Clinical Epidemiology, 103, pp.131–133. doi:10.1016/j.jclinepi.2018.07.01.*

[11] *Song, J., Gu, T., & Mohapatra, P. (2021). How Blockchain Can Help Enhance The Security And Privacy in Edge Computing? arXiv:2111.00416 [cs.CR]. DOI: 10.48550/arXiv.2111.00416.*

[12] *Deng, H., Qin, Z., Wu, Q., et al. (2020). Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. IEEE Transactions on Information Forensics and Security, 15, pp.3168–3180. https://doi.org/10.1109/tifs.2020.298553.*

DOI: 10.54254/2755-2721/145/2025.21867

[13] *Li, J., Zhang, Y., Ning, J., Huang, X., Sen Poh, G., & Wang, D. (2020). Attribute Based Encryption with Privacy protection and Accountability for CloudIoT. IEEE Transactions on Cloud Computing. https://doi.org/10.1109/TCC.2020.2975184.*

[14] *Ullah, I., Amin, N. U., Khan, M. A., Khattak, H., & Kumari, S. (2021). An efficient and provably secure certificate-based combined signature, encryption and signcryption scheme for Internet of Things (IoT) in mobile health (M-health) system. Journal of Medical Systems, 45(1), pp.4–14. https://doi.org/10.1007/s10916-020-01658-.*

[15] *Liu, S., Yu, J., Xiao, Y., Wan, Z., Wang, S., & Yan, B. (2020). BC-SABE: Blockchain-aided searchable attribute-based encryption for cloud-IoT. IEEE Internet of Things Journal 7(9), 7851-7867.*