International Journal of Infrastructure Research and Management
Vol. 11 (2), December 2023, pp. 74- 84

A COMPREHENSIVE SWOT ANALYSIS FOR BLOCKCHAIN-BASED CLOUD DATA INTEGRITY VERIFICATION SCHEME

Li Zhenxiang [1], Jin Yuanrong [1], Wang Haipei [1] & Mohammad Nazir Ahmad [2]
[1]*Infrastructure University Kuala Lumpur, Malaysia*
[2]*Universiti Kebangsaan Malaysia, Malaysia*

ABSTRACT
In the current big data environment where data security is a major concern, the shortcomings of traditional centralised cloud data integrity verification schemes are gradually being identified. These include the lack of transparency in protocol enforcement and the risk of single points of failure. A growing number of researchers have undertaken significant research efforts to address these flaws. To address these challenges, some researchers have proposed a Blockchain-Based Cloud Data Integrity Verification (BBCDIV) scheme by combining blockchain technology with traditional cloud data integrity verification protocols. This paper provides an introduction and a comprehensive SWOT analysis of BBCDIV, a study that aims to assess the strengths, weaknesses, opportunities, and threats of blockchain technology in relation to data integrity in a cloud computing environment. This paper provides an overall view of the BBCDIV solution through an analysis and review of the literature and by considering internal and external factors. The conclusions of this paper highlight the potential advantages of blockchain technology in ensuring secure and reliable data storage and management in cloud environments, while also identifying potential challenges and limitations that need to be addressed for successful implementation. This SWOT analysis can provide a research reference as well as potential future research directions for researchers and practitioners in related fields.

Keywords:
Cloud Storage, Data Security, Integrity Verification, Blockchain, SWOT

INTRODUCTION

In recent years, cloud computing has been more widely used across a wide range of industries as the volume of data has increased dramatically (Oke et al., 2021). Cloud storage, cloud access and cloud management have emerged as a result (Mustafa et al., 2022). However, a number of data security issues, such as data leakage, unauthorised access and tampering (Bandari, 2023) often arise in cloud environments and these serious issues have led to considerable concern about data integrity and security. Various solutions have been proposed to address these challenges, and one very hot solution is the integration of blockchain technology into cloud data integrity verification schemes (He et al., 2021; X. Li et al., 2023; Liu et al., 2023; Yu et al., 2022; C. Zhang et al., 2022; Y. Zhang et al., 2022).

Blockchain was originally introduced as the underlying technology for cryptocurrencies such as Bitcoin and is widely used in finance and IT due to its decentralised and immutable nature (S. N. Khan et al., 2021). It provides a distributed and transparent ledger that enables secure transactions and data storage without the need for a trusted central authority to manage the organisation. Utilizing this feature of the blockchain, the blockchain can provide a technical basis for zero trust (Abdalla et al., 2022). Due to the decentralized and non-tamperable nature of blockchain, it can be used to establish trust and verification mechanisms to ensure the security and authenticity of transactions and information. Blockchain technology can be used for identity verification, data integrity verification, smart contract execution, etc., thereby enhancing the security and credibility of the zero-trust model.

The purpose of this paper is to present a comprehensive SWOT analysis for a blockchain-based cloud data integrity verification scheme. SWOT analysis is a strategic planning tool used to assess the strengths, weaknesses, opportunities and threats associated with a particular initiative (Nyamasvisva et

ISSN Print: 2811-3608
ISSN Online: 2811-3705
https://iukl.edu.my/rmc/publications/ijirm/
DOI:10.63646/j.jdsti.2023110207

al., 2022). In the context of this study, the SWOT analysis provides a systematic assessment of the factors that can influence the success and effectiveness of the proposed programme.
The methodology used for this analysis involved a comparative analysis of relevant literature within the last three years in the relevant field, as well as a thorough review of internal and external factors. Internally, the advantages and disadvantages of a blockchain-based cloud data integrity verification scheme were assessed, considering factors such as scalability, efficiency and usability. Externally, the analysis explores the opportunities and threats associated with the adoption and implementation of the proposed solution, taking into account factors such as regulatory frameworks, market trends and potential security risks.

The findings of this study will clarify the potential advantages of implementing a blockchain-based cloud data integrity verification scheme. It will also highlight the challenges and constraints that need to be addressed to ensure its successful implementation. By providing a comprehensive assessment of the SWOT factors of the scheme, this paper aims to provide valuable insights and guidance to researchers, practitioners and policymakers interested in leveraging blockchain technology for secure and trusted data storage and management in cloud environments.

BACKGROUND

In the big data era, traditional storage technologies suffer from high construction costs, high maintenance difficulties and lack of flexibility (I. Khan et al., 2021), making it difficult to meet large-scale business needs. Cloud computing has emerged as a dominant paradigm for data storage, processing, and service provisioning due to its flexibility, scalability, and cost-effectiveness. To achieve efficient and secure storage and management of big data, more and more users are outsourcing their data to cloud storage. Cloud storage is an extension of cloud computing that uses virtualisation technology to integrate disparate storage devices into a huge pool of storage (Lei et al., 2021), providing users with highly flexible, resource-light, and on-demand rented storage services.

Cloud services allow users to outsource the storage and management of data, significantly reducing the cost of maintaining data. However, data outsourced to the cloud is exposed to many security threats, including data integrity breaches. On the one hand, the insecurity of the cloud storage system itself makes it vulnerable to external attacks such as illegal access, malicious tampering, destruction or deletion; on the other hand, cloud service providers may remove data that is infrequently accessed by users in order to conserve resources and make more profit (Gill et al., 2022).

Therefore, verifying the integrity of outsourced data in cloud storage is one of the keys to ensuring secure data storage and one of the keys to promoting the commercialisation of cloud storage services. The reliance on third-party cloud service providers raises concerns about data integrity, as users have limited control and visibility over their data. The risk of unauthorized access, data tampering, and insider threats has become a major challenge in cloud environments, necessitating robust data integrity verification mechanisms.

Traditional methods of ensuring data integrity, such as checksums and digital signatures, have limitations when it comes to cloud environments (Seth et al., 2022). These approaches typically rely on a centralized authority to verify data integrity, which can be a single point of failure and vulnerable to attacks. Moreover, the lack of transparency and auditability in traditional systems makes it difficult to detect and prove data tampering.

The emergence of blockchain technology in recent years has provided a new direction to address these issues, and a number of studies have combined blockchain with traditional cloud data integrity verification schemes. Blockchain technology has emerged as a potential solution to address these challenges. Originating from the Bitcoin cryptocurrency, blockchain offers a decentralized, tamper-resistant, and transparent mechanism for recording transactions and data. By leveraging the cryptographic properties of blockchain, data can be stored in a distributed ledger, where each transaction is validated

and linked to the previous one, forming an immutable chain of blocks. This decentralized and transparent nature of blockchain ensures data integrity and enhances trust among participants.
Integrating blockchain into cloud data integrity verification schemes can provide several benefits (Whyte et al., 2022). Firstly, it eliminates the need for a centralized authority, reducing the risk of a single point of failure. Secondly, blockchain's immutability ensures that once data is recorded, it cannot be altered or tampered with without consensus from the network. Thirdly, the transparent nature of blockchain allows for easier auditing and verification of data integrity, enhancing trust and accountability.

However, while the potential advantages of blockchain in ensuring cloud data integrity are evident, there are also challenges and limitations that need to be considered. These include scalability issues, high computational requirements, potential privacy concerns, regulatory constraints, and interoperability with existing cloud infrastructure (Habib et al., 2022). Understanding these factors and conducting a comprehensive SWOT analysis is crucial for assessing the feasibility and effectiveness of a blockchain-based cloud data integrity verification scheme.

BBCDIV: A PARADIGM SHIFT IN VERIFICATION TECHNIQUES

Concept Elaboration

Cloud storage provides data owners with flexible resource allocation and ample storage space (Almurisi & Tadisetty, 2022). Data owners no longer need to bear the burden of local data storage but can directly upload their data to cloud storage service providers through network devices. The service providers then manage the data and allocate storage space as needed, optimizing storage resource utilization. However, cloud storage also means that data owners lose direct control over their data, resulting in a lack of effective security and accuracy guarantees for cloud data. On the one hand, cloud storage service providers may delete data resources with low access rates to improve storage space utilization. On the other hand, untrusted cloud storage service providers may collude with adversaries to leak remote data for profit. To ensure the security of cloud data, integrity verification technology has emerged.

With the help of this technology, data owners can check the integrity of remote data without having to download the complete files (Han et al., 2022). As shown in Figure 1, data owners usually upload their data to cloud storage servers to reduce storage costs. They also employ third-party auditors to perform integrity audits on the cloud data and receive the verification results. When the verification results indicate incompleteness, it implies that malicious activities such as data loss or damage have occurred to the remote data. In such cases, data owners can hold the cloud storage service provider accountable.

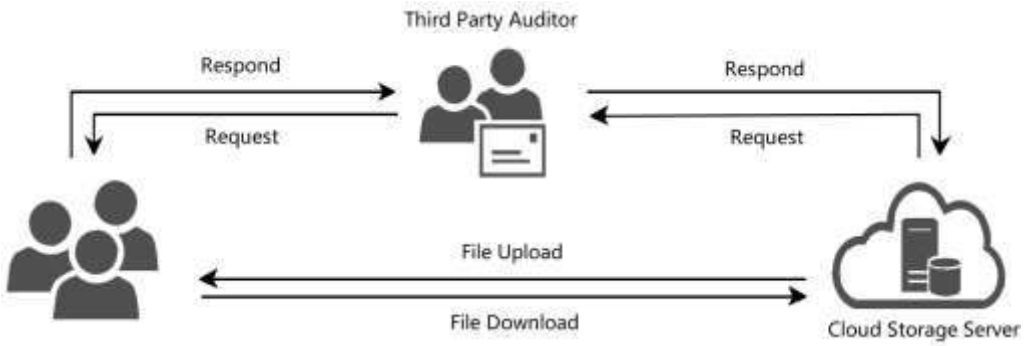

Figure 1. Integrity Verification Model for Cloud Data

Attack Model

In the cloud data integrity verification model, although third-party auditors can effectively assist data owners in performing integrity audits on remote data, the introduction of untrusted third-party auditors increases the risk of cloud data leakage (Razaque et al., 2021). Collusion attacks pose the most significant threat to existing cloud data integrity verification models. These attacks involve collusion between the cloud storage server and adversaries, collusion between the third-party auditor and adversaries, as well as collusion among the cloud storage server, the third-party auditor, and adversaries. Such malicious activities can result in data breaches or direct secondary attacks on cloud data, such as forgery, tampering, or substitution attacks.

Specifically, when the malicious cloud storage service provider receives data uploaded by the data owner, it performs illegal operations on the uploaded data (Wang et al., 2022). For example, it may forge new data content based on the uploaded data, tamper with a portion of the uploaded data, or replace the original data with other users' data. Ultimately, the untrusted third-party auditor generates verification results based on incorrect data content, leading the data owner to believe that the erroneous data content is the original data uploaded. This attempt aims to deceive the data owner and other users who download the data.

Technical Realization

The integrity verification protocol is a challenge-response interactive algorithm run by the verifier (i.e., the third-party auditor) and the cloud storage server (Rehman et al., 2021). It mainly consists of three stages: the challenge stage, the proof stage, and the verification stage. Unlike the ownership proof protocols mentioned above, the integrity verification protocol is verifier-centric, requiring the cloud storage server to generate correct responses in order to meet the verifier's challenges.

Challenge Stage: Assuming the data content is F, the verifier randomly generates a challenge value Chal based on the data content F and sends it to the cloud storage server.

- Proof Stage: The cloud storage server receives the challenge value Chal and computes a proof value Proof regarding the data content F stored. The server then returns the proof value Proof to the verifier.
- Verification Stage: The verifier runs the CheckProof(Proof) function to verify the correctness of the proof value and further determine the integrity of the data content F. Here, CheckProof(.) is a cryptographic verification algorithm.

The formal definition of the integrity verification protocol is as follows:

- (pk,sk) ← PkeyGen(1^λ): Public-private key generation algorithm. It takes a security parameter 1λ as input and outputs the public key pk and private key sk.
- φ ← HtagGen(pk,sk,C): Homomorphic signature generation algorithm. It takes a public key pk, private key sk, and ciphertext C as input and outputs the corresponding homomorphic signature φ.
- P ← GenProof(C,Chal,σ): Proof generation algorithm. It takes a ciphertext C, challenge Chal, and homomorphic signature φ as input and outputs the corresponding proof P.
- V ← CheckProof(pk,sk,Chal,P): Verification algorithm. It takes a public key pk, private key sk, challenge Chal, and proof P as input and outputs the corresponding verification value V, where V = 1 indicates successful verification, and V = 0 indicates verification failure.

To meet the requirements of data integrity verification in different application scenarios, researchers have made supplementary and improved algorithms based on the aforementioned foundational algorithms to adapt to specific scenario requirements (Ding et al., 2020; Gudeme et al., 2021).

BBCDIV STRENGTHS

BBCDIV has a number of distinct advantages over traditional validation methods. The key strengths of BBCDIV are outlined in Table 1.

Table 1. The Strengths of BBCDIV

No	Strength	Explanation
1	Decentralization and Trust	BBCDIV takes advantage of the decentralised nature of blockchain technology, eliminating the possibility of fraud by a centralised institution or any trusted third party. This decentralisation promotes trust between participants by ensuring that no single entity has control over the validation process. It reduces the risk of manipulation or tampering and increases the overall trustworthiness of the system.
2	Tamper-Proof Data Storage	The immutability and tamper-proof nature of blockchain form a strong foundation for data integrity verification in BBCDIV. Once data is recorded in the blockchain, it becomes virtually impossible to alter or tamper with without consensus from the network participants. This ensures the integrity and authenticity of cloud-stored data, providing a reliable and auditable record.
3	Transparency and Auditability	BBCDIV provides transparency and auditability of the cloud data validation process. Every transaction recorded in the blockchain is visible to all participants, promoting transparency and making the integrity of the data easily auditable. This transparency enhances trust between users and allows real-time verification of data, promoting traceability accountability.
4	Enhanced Security	The application of cryptographic algorithms in BBCDIV enhances the security of cloud data integrity verification. The decentralised nature of the blockchain reduces the risk of a single point of failure and makes the system more defensible against attacks.
5	Collaborative Verification	BBCDIV enables enhanced collaboration between cloud service providers, users and blockchain network participants. By involving multiple entities in the validation process, BBCDIV distributes responsibility and increases the overall trust in the system.

These advantages enable BBCDIV to be a more secure and reliable solution for verifying the integrity of data stored in the cloud. By leveraging the decentralised, tamper-proof, transparent and collaborative nature of blockchain, BBCDIV provides enhanced security, trust and traceability mechanisms.

BBCDIV WEAKNESSES

While BBCDIV, a blockchain-based cloud data integrity verification solution, has significant advantages, it is not free from concerns and it must be acknowledged that it also has some weaknesses and potential limitations. Understanding these weaknesses is essential to fully assess the viability and effectiveness of BBCDIV. Table 2 shows some of the possible weaknesses associated with BBCDIV.

Table 2. The Weaknesses of BBCDIV

No	Weakness	Explanation
1	Scalability Challenges	One of the main challenges of blockchain technology is its scalability. BBCDIV inherits this same potential weakness, with the size of the blockchain growing as the number of transactions increases, leading to potential performance bottlenecks. The validation process can become time-consuming and resource-intensive, affecting the overall efficiency of BBCDIV, especially in high-volume cloud environments.
2	Computational Requirements	Blockchain networks rely on consensus mechanisms, which often require significant computing power and energy consumption. This can create many obstacles, especially for organisations with limited computing resources.
3	Potential Security Risks	While blockchain technology itself is known for its security features, BBCDIV may still be exposed to security risks at different levels. These risks include vulnerabilities in the underlying blockchain infrastructure, potential attacks against consensus algorithms, or security weaknesses in the implementation of validation schemes.
4	Regulatory Considerations	The adoption of BBCDIV may raise regulatory and legal concerns. Blockchain technology is relatively new and rapidly evolving, and the regulatory framework is still under development.

Understanding and addressing these weaknesses will allow the potential of BBCDIV to be better utilised. This still requires further research and development work to overcome these challenges in order to achieve effective and secure cloud data integrity verification. By acknowledging these weaknesses and working to address them, BBCDIV can evolve into a more robust and practical solution for ensuring data integrity in cloud computing environments.

BBCDIV OPPORTUNITIES

BBCDIV can further increase its effectiveness, adoption and impact in the cloud computing space. These opportunities arise from the unique advantages of blockchain technology, which addresses some of the limitations of traditional integrity verification schemes. Table 3 shows the possible opportunities associated with BBCDIV.

Table 3. The Opportunities of BBCDIV

No	Opportunities	Explanation
1	Enhanced Data Governance	BBCDIV provides an opportunity to strengthen data governance practices in cloud computing environments. The decentralized and transparent nature of blockchain ensures greater accountability and traceability of data transactions. Organizations can leverage BBCDIV to demonstrate compliance with data integrity and privacy regulations, enhance their reputation, and build trust with customers and stakeholders.
2	Integration with Internet of Things (IoT)	The proliferation of IoT devices generates vast amounts of data (Fatin et al., 2022) that require secure and trustworthy storage and verification. BBCDIV can be integrated with IoT systems, enabling reliable and transparent data integrity verification for IoT-generated

		data. This integration opens up opportunities for applications in various sectors, such as healthcare, supply chain management, and smart cities.
3	Collaboration among CSPs	BBCDIV promotes collaboration among cloud service providers (CSPs) in maintaining the integrity of data stored in the cloud. CSPs can establish consortia or partnerships to collectively implement BBCDIV, thereby enhancing the overall trustworthiness of their services. Collaboration in data integrity verification can lead to shared best practices, interoperability standards, and improved security measures within the cloud ecosystem.
4	Development of Customized Verification Schemes	BBCDIV can be customized and tailored to specific industry requirements and use cases. Different sectors, such as finance, healthcare, or legal services, may have unique data integrity verification needs. Organizations can explore opportunities to develop specialized verification schemes using BBCDIV that cater to their specific industry requirements, ensuring compliance, security, and efficiency.
5	Integration with Artificial Intelligence (AI) and Machine Learning (ML)	The integration of AI and ML techniques with BBCDIV can enhance the efficiency and accuracy of data integrity verification. AI algorithms can analyze patterns and detect anomalies in the blockchain, enabling automated detection of potential data integrity breaches. ML models can continuously learn from verified data, improving the overall reliability and effectiveness of the verification process.

By leveraging these opportunities, researchers and practitioners can further develop and refine BBCDIV into a more advanced cloud data integrity verification solution. These opportunities enable continued innovation, collaboration and adoption of blockchain-based solutions to drive the transformation of cloud data integrity verification and unlock new possibilities in secure and trusted cloud computing environments.

BBCDIV THREATS

While BBCDIV, a blockchain-based cloud data integrity verification solution, offers significant benefits and opportunities, it is important to consider the potential threats and challenges that may hinder its adoption and effectiveness. Identifying and addressing these threats is critical to the successful implementation and utilisation of BBCDIV. Table 4 shows the main threats associated with BBCDIV.

Table 4. The Threats of BBCDIV

No	Threats	Explanation
1	Regulatory and Legal Challenges	The regulatory landscape around blockchain technology is still evolving and compliance with existing and future regulations may pose challenges to the implementation of BBCDIV. Ambiguities in data protection, privacy and intellectual property laws may create legal uncertainty and barriers to adoption.
2	Energy Consumption and	Blockchain networks, particularly those utilising proof-of-work consensus mechanisms, require significant computing power and energy consumption. The environmental impact of such energy-

	Environmental Impact	intensive operations is a growing concern, particularly in regions with strict environmental regulations or sustainability goals.
3	Scalability and Performance Limitations	Blockchain technology currently faces scalability limitations, especially when dealing with large numbers of transactions. As the blockchain grows, the validation process can become slow and resource intensive, impacting the overall performance and efficiency of BBCDIV.
4	Security Vulnerabilities and Attacks	Despite the inherent security features of blockchain technology, BBCDIV is not immune to security vulnerabilities and potential attacks. Vulnerabilities in smart contracts, consensus attacks or malicious activity against the blockchain network can compromise the integrity of the authentication process.
5	Economic and Cost Considerations	There may be significant costs involved in implementing BBCDIV and maintaining a blockchain network, including infrastructure setup, network maintenance and computing resources. The economic viability of BBCDIV may be influenced by factors such as cost effectiveness and return on investment.

By recognizing and addressing these threats, researchers, practitioners, and policymakers can work towards developing strategies and solutions to mitigate risks and enhance the effectiveness of BBCDIV. Collaborative efforts, industry standards, regulatory support, and ongoing research are vital for navigating the threats associated with BBCDIV and ensuring its successful implementation as a robust cloud data integrity verification scheme.

CONCLUSION

Combining blockchain technology with cloud data integrity verification can improve the reliability and stability of integrity verification protocols, eliminate the risk of single point of failure, and also make the operation of the protocol open and transparent, so that when the protocol is executed abnormally, it can be traced back to the party that violated it. Blockchain can provide a practical and effective solution to some of the inherent flaws of traditional centralised TPA-based integrity verification schemes, and has great application potential and research value (Wu et al., 2023).

In this paper, we present a comprehensive SWOT analysis of BBCDIV, a blockchain-based integrity verification scheme for cloud data. The analysis highlights the strengths, weaknesses, opportunities and threats associated with BBCDIV, providing a comprehensive view of its potential to ensure data integrity in a cloud computing environment. Table 5 summarises the strengths, weaknesses, opportunities and threats of adopting BBCDIV as an existing cloud data integrity validation solution.

Table 5. SWOT analysis of the BBCDIV

Strengths	**Weaknesses**
• Decentralization and Trust • Tamper-Proof Data Storage • Transparency and Auditability • Enhanced Security • Collaborative Verification	• Scalability Challenges • Computational Requirements • Potential Security Risks • Regulatory Considerations

Opportunities	**Threats**
• Enhanced Data Governance • Integration with Internet of Things • Collaboration among CSPs • Development of Customized Verification Schemes • Integration with Artificial Intelligence (AI) and Machine Learning (ML)	• Regulatory and Legal Challenges • Energy Consumption and Environmental Impact • Scalability and Performance Limitations • Security Vulnerabilities and Attacks • Economic and Cost Considerations

AUTHOR BIOGRAPHY

Li Zhenxiang is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. His research interests include Blockchain, Cloud Computing and Data Integrity Verification. *Email: 222923380@s.iukl.edu.my*

Jin Yuanrong is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. Her research interests include Cloud Computing and Load Prediction algorithms. *Email: 222923382@s.iukl.edu.my*

Wang Haipei is student of the postgraduate programme PhD (Information Technology) at Infrastructure University Kuala Lumpur (IUKL) Faculty of Engineering, Science and Technology. Her research interests include Cloud Computing and cyber security *Email: 223923726@s.iukl.edu.my*

Mohammad Nazir Ahmad AP. Dr, is an Associate Professor at Universiti Kebangsaan Malaysia (UKM) specializing in Ontology and Knowledge Management. He has a PhD in Information Technology, received substantial research grants, published extensively, and supervised multiple academic projects. He is actively involved in international associations and organizations related
to his field. *Email: mnazir@ukm.edu.my*

REFERENCES

Abdalla, A., Arabi, M., Nyamasvisva, T. E., & Valloo, S. (2022). ZERO TRUST SECURITY IMPLEMENTATION CONSIDERATIONS IN DECENTRALISED NETWORK RESOURCES FOR INSTITUTIONS OF HIGHER LEARNING. *International Journal of Infrastructure Research and Management*, *10*(1), 79–90. https://iukl.edu.my/rmc/publications/ijirm/

Almurisi, N., & Tadisetty, S. (2022). Cloud-based virtualization environment for IoT-based WSN: solutions, approaches and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *13*(10), 4681–4703. https://doi.org/10.1007/S12652-021-03515-Z/TABLES/5

Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), 1–11. https://research.tensorgate.org/index.php/IJBIBDA/article/view/3

Ding, R., Xu, Y., Cui, J., & Zhong, H. (2020). A Public Auditing Protocol for Cloud Storage System with Intrusion-Resilience. *IEEE Systems Journal*, *14*(1), 633–644. https://doi.org/10.1109/JSYST.2019.2923238

Fatin, F., Majid, S., Syafiq, M., & Mohamed, N. (2022). DEVELOPMENT OF SURVEILLANCE SYSTEM WITH AUTOMATED EMAIL AND TELEGRAM NOTIFICATION USING OPEN-SOURCE APPLICATION PROGRAMMING INTERPHASE (API). *International Journal of*

Infrastructure Research and Management, *10*(2), 39–49. https://iukl.edu.my/rmc/publications/ijirm/

Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S. K., Baker, T., Parlikad, A. K., Lutfiyya, H., Kanhere, S. S., Sakellariou, R., Dustdar, S., … Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. *Internet of Things*, *19*, 100514. https://doi.org/10.1016/J.IOT.2022.100514

Gudeme, J. R., Pasupuleti, S. K., & Kandukuri, R. (2021a). Attribute-based public integrity auditing for shared data with efficient user revocation in cloud storage. *Journal of Ambient Intelligence and Humanized Computing*, *12*(2), 2019–2032. https://doi.org/10.1007/S12652-020-02302-6/METRICS

Gudeme, J. R., Pasupuleti, S. K., & Kandukuri, R. (2021b). Certificateless multi-replica public integrity auditing scheme for dynamic shared data in cloud storage. *Computers & Security*, *103*, 102176. https://doi.org/10.1016/J.COSE.2020.102176

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet 2022, Vol. 14, Page 341*, *14*(11), 341. https://doi.org/10.3390/FI14110341

Han, H., Fei, S., Yan, Z., & Zhou, X. (2022). A survey on blockchain-based integrity auditing for cloud data. *Digital Communications and Networks*, *8*(5), 591–603. https://doi.org/10.1016/J.DCAN.2022.04.036

He, K., Huang, C., Shi, J., Hu, X., & Fan, X. (2021). Enabling Decentralized and Dynamic Data Integrity Verification for Secure Cloud Storage via T-Merkle Hash Tree Based Blockchain. *Mobile Information Systems*, *2021*. https://doi.org/10.1155/2021/9977744

Khan, I., Baig, N., Ali, S., Usman, M., Khan, S. A., & Saeed, K. (2021). Progress in layered cathode and anode nanoarchitectures for charge storage devices: Challenges and future perspective. *Energy Storage Materials*, *35*, 443–469. https://doi.org/10.1016/J.ENSM.2020.11.033

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901–2925. https://doi.org/10.1007/S12083-021-01127-0/FIGURES/4

Lei, N., Chong, H., & Zhang, Y. (2021). Cloud Computing Technology in the Construction of Intelligent Campus. *Lecture Notes in Electrical Engineering*, *747*, 2147–2152. https://doi.org/10.1007/978-981-16-0115-6_258/FIGURES/1

Li, J., Tan, X., Chen, X., & Wong, D. S. (2013). An efficient proof of retrievability with public auditing in cloud computing. *Proceedings - 5th International Conference on Intelligent Networking and Collaborative Systems, INCoS 2013*, 93–98. https://doi.org/10.1109/INCOS.2013.185

Li, X., Yi, Z., Li, R., Wang, X.-A., Li, H., & Yang, X. (2023). SM2-Based Offline/Online Efficient Data Integrity Verification Scheme for Multiple Application Scenarios. *Sensors 2023, Vol. 23, Page 4307*, *23*(9), 4307. https://doi.org/10.3390/S23094307

Liu, Z., Ren, L., Feng, Y., Wang, S., & Wei, J. (2023). Data Integrity Audit Scheme Based on Quad Merkle Tree and Blockchain. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3240066

Mustafa, M., Alshare, M., Bhargava, D., Neware, R., Singh, B., & Ngulube, P. (2022). Perceived Security Risk Based on Moderating Factors for Blockchain Technology Applications in Cloud Storage to Achieve Secure Healthcare Systems. *Computational and Mathematical Methods in Medicine*, *2022*. https://doi.org/10.1155/2022/6112815

Nyamasvisva, T. E., Abdalla, A., & Arabi, M. (2022). A COMPREHENSIVE SWOT ANALYSIS FOR ZERO TRUST NETWORK SECURITY MODEL. *International Journal of Infrastructure Research and Management*, *10*(1), 44–53. https://iukl.edu.my/rmc/publications/ijirm/

Oke, A. E., Kineber, A. F., Albukhari, I., Othman, I., & Kingsley, C. (2021). Assessment of Cloud Computing Success Factors for Sustainable Construction Industry: The Case of Nigeria. *Buildings 2021, Vol. 11, Page 36*, *11*(2), 36. https://doi.org/10.3390/BUILDINGS11020036

Razaque, A., Frej, M. B. H., Alotaibi, B., & Alotaibi, M. (2021). Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey. *Electronics 2021, Vol. 10, Page 2721*, *10*(21), 2721. https://doi.org/10.3390/ELECTRONICS10212721

Rehman, A., Jian, L. I. U., Yasin, M. Q., & Keqiu, L. I. (2021). Securing Cloud Storage by Remote Data Integrity Check with Secured Key Generation. *Chinese Journal of Electronics*, *30*(3), 489–499. https://doi.org/10.1049/CJE.2021.04.002

Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecommunications Technologies*, *33*(4), e4108. https://doi.org/10.1002/ETT.4108

Wang, J., Wang, S., Wang, L., Shao, W., Xu, S., & Zhang, S. (2022). A Blockchain and Edge Computing Based Public Audit Scheme for Cloud Storage. *Chinese Control Conference, CCC*, *2022-July*, 7466–7470. https://doi.org/10.23919/CCC55666.2022.9902871

Whyte, S. T., Omoyiola, B. O., & Okoni, B. (2022). Use of Blockchain Technology in Data Integrity Assurance. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.4043164

Wu, D., Yang, Z., Zhang, P., Wang, R., Yang, B., & Ma, X. (2023). Virtual-Reality Inter-Promotion Technology for Metaverse: A Survey. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2023.3265848

Yu, H., Yang, Z., Tu, S., Waqas, M., & Liu, H. (2022). Blockchain-Based Offline Auditing for the Cloud in Vehicular Networks. *IEEE Transactions on Network and Service Management*, *19*(3), 2944–2956. https://doi.org/10.1109/TNSM.2022.3164549

Zhang, C., Xu, Y., Hu, Y., Wu, J., Ren, J., & Zhang, Y. (2022). A Blockchain-Based Multi-Cloud Storage Data Auditing Scheme to Locate Faults. *IEEE Transactions on Cloud Computing*, *10*(4), 2252–2263. https://doi.org/10.1109/TCC.2021.3057771

Zhang, Y., Geng, H., Su, L., & Lu, L. (2022). A Blockchain-Based Efficient Data Integrity Verification Scheme in Multi-Cloud Storage. *IEEE Access*, *10*, 105920–105929. https://doi.org/10.1109/ACCESS.2022.3211391