https://doi.org/10.56861/inheriten.v1i1
e-ISSN: 0000-0000

International Journal of Informatics, High-End Research, Innovation, and Emerging Technologies
Inheriten Journal
Vol. 1, No. 1, January 2026 pp. 1-11
Journal Page is available at https://internationaljournal.lppmunsaka.ac.id/index.php/inheriten

Comparative Study of Data Security: Cloud Storage and Local Storage in Technology Companies

Neng Wiwin[1], Teddy Hidayat[2], Siti Nur Aisyah Rahman[3]
[1]Universitas Salakanagara, Indonesia
[2]Universitas Muhammadiyah Bandung, Indonesia
[3]Universiti Malaya, Malaysia
Email: nengwiwin@unsaka.ac.id

Abstract

In the era of digital transformation, data security has become a top priority for technology companies. This study presents a comparative analysis of cloud storage and local storage, emphasizing their respective security implications. Cloud storage offers scalability, remote accessibility, and cost-efficiency but raises concerns related to data control and vulnerability to cyber threats. Conversely, local storage provides direct data governance and enhanced access speed, albeit at the cost of limited scalability and higher infrastructure investment. Through literature analysis and synthesis of current research, the study identifies hybrid and local-first storage models as viable alternatives to balance security, performance, and scalability. The findings highlight that the best strategy for technology enterprises lies in adopting a risk-based approach to storage architecture that integrates strong security protocols, real-time control mechanisms, and infrastructure optimization.

Keywords: Cloud Storage; Local Storage; Data Security; Hybrid Model; Local-First Architecture; Cybersecurity; Access Control; Scalability; Performance

INTRODUCTION

Data storage has become one of the most important aspects of a technology company's operations. As the amount of data generated increases, companies must decide on the most effective and secure storage method. Cloud storage and on-premises storage are two primary methods that are often considered. While both have their own advantages and disadvantages, data security remains a primary concern when choosing a storage method. In a data-driven digital era, technology companies face complex challenges in managing and protecting their valuable information assets. Data security is a top priority, with significant implications for reputation, regulatory compliance and business sustainability.(Shengbin, 2020). The two main approaches to data storage, cloud storage and local storage, offer different advantages and disadvantages in terms of security, cost, scalability, and performance. Enterprises are increasingly evaluating the benefits of cloud services.(Asniar & Sari, 2015). However, this use comes with security risks and potential data leaks.(Jeevitha et al., 2016; Kanatt et al., 2020). A deep understanding of the security differences between these two storage models is critical for technology companies to make informed decisions and implement effective data protection strategies.(Rahman et al., 2023).

Cloud storage, with distributed infrastructure and services managed by third-party providers, offers attractive scalability, flexibility, and cost efficiency.(Dawood et al., 2023). However, this model also raises concerns about data control, privacy, and potential vulnerability to cyberattacks.(Kulkarni et al., 2012). Local storage, on the other hand, gives companies direct control over their data and infrastructure, but requires significant investment in hardware, software, and security experts. Information system security is very important for an institution to maintain information optimally and safely.(Umar et al., 2019). Maintaining integrity requires not only system-level access controls, but also ensuring that system users can

only change data that they are legally permitted to change.(Paryati, 2015). In addition, in some cases, it is important to ensure that every action taken by a user is regularly recorded and that these records are protected from unauthorized access or alteration.(Saputra et al., 2023). Companies that store data locally can choose to implement encryption and access control strategies that suit their specific needs. The protection of critical data and assets can be enhanced by adopting a comprehensive approach to cybersecurity, and organizations should also take steps to mitigate the risk of cyberattacks.(Herdiana et al., 2021).

Although many studies have discussed the advantages of each storage system, in-depth analysis of data security focusing on technology companies is still rare. This study aims to conduct an in-depth comparative study of data security in cloud storage and local storage, focusing on technology companies.

LITERATURE REVIEW

Cloud storage has become increasingly popular in recent years due to its scalability, flexibility, and cost-efficiency. Cloud storage providers offer a variety of services, including data storage, backup, and disaster recovery. However, cloud storage also poses some security concerns. Cybercrime is becoming more common as the internet continues to function as a hub for commerce, entertainment, and government tools.(Idellie & Atok, 2023). Therefore, the internet environment opens up new avenues for the emergence of criminal acts.(Chintia et al., 2019). One of the main concerns is data control. When companies store data in the cloud, they hand over control of that data to the cloud service provider. This can raise concerns about data privacy, compliance, and potential unauthorized access to data.(Anggraeni, 2018). On-premises storage, on the other hand, gives businesses direct control over their data and infrastructure. This model involves storing data on servers and hardware located within the company's physical premises. This allows businesses to implement security measures that suit their specific needs and ensure that their data remains under their control at all times.

Data security is an important aspect of both storage methods. Virtual information identities are collections of numbers and identifiers in computer databases owned by governments and digital companies that collect various inputs.(Idellie & Atok, 2023). Therefore, these identities are at risk of being stolen, misused, or forged. Companies must take steps to protect their data from unauthorized access, data leaks, and other cyber threats.(Asaad & Saeed, 2022). One of the most important security measures is encryption. Encryption converts data into an unreadable format, making it inaccessible to unauthorized persons. Encryption can be used to protect data in transit and at rest. Traditional methods for data security usually rely on data encryption and access control. Encrypting data with AES or other encryption methods will prevent valuable information from leaking even if an adversary obtains the data. However, it has efficiency issues when dealing with oceans of data in cloud environments due to the large encryption and decryption overhead in storage and computing.(Commey et al., 2020; Shi, 2018).

METHODOLOGY

This study will use a qualitative approach to collect and analyze data. The collected data will be analyzed using statistical analysis and content analysis to identify trends, patterns, and significant differences in data security between cloud storage and local storage. Qualitative research is conducted by interpreting the data that has been obtained.(Rutania & Ganggi, 2021). In qualitative research, data collection is a very important step to achieve research objectives.(Fauziah & Apriani, 2021; Latifah & Abdullah, 2024). Research data was collected using literature study, observation, and documentation methods. In analyzing this research, namely qualitative, qualitative analysis techniques are research that provides descriptive legal material results in the form of written words.(Fauziah & Apriani, 2021). Qualitative analysis

provides an accurate description and interpretation of the meaning of a symptom that occurs in a social context.(Setiawan et al., 2020). By using the library research method, library data in the form of journals, books, and documents, both printed and electronic, as well as other data sources that are considered relevant to this study are collected.(Assyakurrohim et al., 2022; Pratiwi & Sari, 2019). Library research is a series of activities related to the method of collecting library data, then read, recorded, and processed into research materials. The research method used in this study is the normative legal research method, namely research that refers to legal norms contained in laws and literature.(Brilliana, 2022).

RESULTS

Here is a comparative analysis of the latest studies and sources on data security: Cloud Storage vs Local Storage in technology companies:

1. Definition & Ownership Model

Cloud storage is a data storage system distributed across multiple computers that work together to store files optimally (Alizadeh & Karimpour, 2014). This allows users to store and access their data anytime and anywhere via the internet. Some of the advantages of cloud storage include high scalability, low cost, and ease of access ("Analysis of Cloud Computing and Cloud Storage in Mobile Forensics Using the DEMATEL Method", 2024). However, cloud storage also has challenges related to data security and privacy (Kumar & Nagalakshmi, 2019; Yang et al., 2020).

On the other hand, local storage is data storage managed locally on the user's device (Tudoran et al., 2013). Local storage has higher I/O performance than cloud storage, but its storage capacity is limited (Ács et al., 2013). In addition, local storage requires more complex management and maintenance by the user (Eyers et al., 2011). To overcome their respective limitations, some studies have proposed a hybrid model that integrates cloud storage and local storage (Xu et al., 2021; Zhang et al., 2018). With this model, data can be stored in local storage for better performance, while cloud storage is used for scalability and backup (Xu et al., 2022). In terms of ownership model, cloud storage is generally owned and managed by the cloud service provider, while users only rent storage space (Mahendar & Chatrapati, 2015; Yang et al., 2020). This raises challenges regarding user control and data security (Aziz & Mahmood, 2022). In contrast, local storage is fully owned and managed by the user, providing greater control but also greater responsibility (Zeng & Zhao, 2013).

Several studies have proposed schemes to improve security and transparency in cloud storage, such as the use of encryption (Peng, 2014; Zhang et al., 2015), blockchain (Aguru et al., 2024; Huang et al., 2020), and public verification (Gao et al., 2020; Yang et al., 2019). In addition, deduplication techniques (Shyamala & S., 2015; Haoran et al., 2015) and hierarchical coding Yang et al. (2019) have also been proposed to improve storage efficiency in the cloud. Overall, cloud storage and local storage have their own advantages and disadvantages, making a hybrid model that integrates both a promising solution. However, challenges related to security, privacy, and data control still need to be addressed to ensure safe and efficient storage usage.

2. Security & Control

Cloud storage offers ease of access and high scalability, but also poses challenges related to data security and control Yahya et al. (2019)(Vimal, 2019; Wu et al., 2019; . Data storage in the cloud is vulnerable to threats such as hacking, unauthorized access, and data theft (Vimal, 2019; Wu et al., 2019; Zhang et al., 2023). This is due to the separation between data ownership and management, so that users lose direct control over their data (Gudimetla, 2024). To address security issues, various techniques have been proposed, such as encryption (Gudimetla, 2024; Yu et al., 2016; El-Booz et al., 2016), blockchain (Aguru et al., 2024), and public verification (Gao et al., 2020). These techniques aim to improve the confidentiality, integrity, and

Vol. 1, No. 1, January 2026, pp. 1-11
https://doi.org/10.56861/inheriten.v1i1.174

transparency of data stored in the cloud (Sheela, 2022). In addition, stricter access controls are also needed to limit access to authorized users only (Niu, 2017).

On the other hand, local storage provides users with greater control over their data (Tudoran et al., 2013; (Ács et al., 2013). However, local storage also has challenges related to more complex management and maintenance (Eyers et al., 2011). In addition, local storage capacity is limited and its I/O performance varies depending on the system used, but can generally be lower than cloud storage (Ács et al., 2013). To integrate the advantages of cloud storage and local storage, some studies have proposed a hybrid model that utilizes both (Xu et al., 2021; (Xu et al., 2022). In this model, data can be stored in local storage for better performance, while cloud storage is used for scalability and backup (Xu et al., 2022). Overall, both cloud storage and on-premises storage have challenges related to data security and control that must be addressed. The use of advanced security techniques, strict access control, and hybrid models can be promising solutions to improve data security and control in cloud and on-premises storage.

Comparison of Security Aspects between Storage Methods

Security Aspect	Cloud Storage	Local Storage
Data Control	Limited to the provider	Full control by the company
Security Threats	Vulnerable to cyberattacks	Lower risk from external threats
Physical Security	Servers are located at the provider’s facilities	Servers are located on company premises
	Dependent on the provider’s compliance standards	Easier to comply with local regulations

3. Reliability & Redundancy

Cloud storage offers high reliability through data redundancy Feng et al. (2012) Kang et al., 2014; (Li et al., 2016; . Cloud storage systems generally use replication and erasure coding techniques to improve data availability and resilience (Heo et al., 2016; (Rodrigues et al., 2013; Xu & Bhalerao, 2015). Data replication across multiple cloud locations can improve reliability by reducing the risk of data loss due to a single server failure (Li et al., 2016; Xu & Bhalerao, 2015). In addition, error coding can also reduce storage overhead compared to simple replication (Rodrigues et al., 2013; (Mandava & Xing, 2017). On the other hand, local storage has lower reliability due to limited redundancy (Tudoran et al., 2013; Ács et al., 2013). However, local storage can offer higher I/O performance than cloud storage (Tudoran et al., 2013; Ács et al., 2013). To improve the reliability of local storage, some studies have proposed schemes such as RAID (Redundant Array of Independent Disks) (O'Neill & Soh, 2023; Song et al., 2015).

To integrate the advantages of cloud storage and local storage, several hybrid models have been proposed (Xu et al., 2021; Zhang et al., 2018). In these models, data can be stored in local storage for better performance, while cloud storage is used for redundancy and backup (Xu et al., 2022). Data deduplication techniques can also be used to improve storage efficiency in hybrid models (Li et al., 2015; Zhu et al., 2014). In addition, cloud storage reliability can also be improved through techniques such as hierarchical coding (Yang et al., 2019), public verification (Gao et al., 2020; Yang et al., 2019), and blockchain (Aguru et al., 2024; Huang et al., 2020). These techniques aim to improve the reliability, transparency, and security of data

stored in the cloud (Mandava & Xing, 2017; Jiang & Zhang, 2017). Overall, cloud storage offers higher reliability through data redundancy, while local storage has better I/O performance but lower reliability. A hybrid model that integrates the two can be a promising solution to gain the advantages of both types of storage.

4. Accessibility & Performance

Cloud storage offers very high accessibility, allowing users to access and manage data from multiple locations as long as there is an internet connection. This greatly supports collaboration and remote work, as demonstrated by services such as Dropbox and OneDrive that facilitate efficient file synchronization and sharing across multiple devices (Daher & Hajjdiab, 2018; Alotaibi et al., 2019). In contrast, local storage is limited to physical devices and can only be accessed at specific locations. However, this solution is ideal for environments with limited internet connectivity or that require physical control over data. In terms of performance, cloud storage has a performance that is highly dependent on the quality of the internet connection and the service provider. Studies show that Nextcloud outperforms Owncloud in terms of file upload and download speeds (Haryani et al., 2024). In addition, cloud service providers often use techniques such as data deduplication and load balancing to improve system efficiency (Gavali et al., 2014). Meanwhile, local storage offers higher access speeds and lower latency due to direct connections to hardware, making it a superior solution for applications that require fast and stable data access. Local storage performance is also more consistent because it is not affected by network variability. Thus, while cloud storage excels in terms of flexibility and remote access, local storage remains the primary choice in contexts that demand speed and full control over data. The choice between the two largely depends on the user's needs and their respective operational environments.

5. Scalability & Cost

Cloud storage stands out in terms of scalability, allowing organizations to easily and quickly expand their storage capacity as data needs grow. These solutions offer virtually unlimited capacity without requiring a large initial investment (Malaiyappan et al., 2024), and support dynamic scaling that allows businesses to adjust resources in real-time (Kanumuri, 2024). On the other hand, on-premises storage is limited by physical hardware capacity, and its expansion requires significant investment in additional devices and supporting infrastructure ("Building a Fast and Efficient LSM-tree Store by Integrating Local Storage with Cloud Storage", 2022). However, on-premises storage tends to provide higher access speeds, making it an ideal solution for applications with high-performance demands.

In terms of cost, cloud storage offers low upfront costs, making it attractive to many organizations looking to avoid large capital outlays. However, ongoing operational costs can add up over time if not managed efficiently (Kanumuri, 2024). Cloud storage is also more cost-effective in large-scale data scenarios and can provide efficiencies through the use of tiered storage solutions. In contrast, on-premises storage demands higher upfront costs for hardware purchases and maintenance, but offers more predictable long-term costs (Goncalves et al., 2018). This approach is also more suitable for small-scale environments with high performance needs, where operational costs can be lower over time. Overall, while cloud storage excels in scalability and flexibility, on-premises storage remains an important option for organizations that prioritize speed of access and cost stability. The decision between these two models is largely influenced by an organization’s specific needs and data usage patterns.

6. Hybrid & Local-First Model

The hybrid model combines local and cloud storage to optimize data access and cost efficiency. This approach enables flexible data management by leveraging local storage for fast access and cloud storage for high scalability (Samy et al., 2017). Cost efficiency is one of the main advantages of this model, as implemented in systems such as HyCloud that effectively balance file system performance and low storage costs (E et al., 2019). In addition, the use of

techniques such as sharding and intelligent data redundancy in the hybrid model can improve performance and fault tolerance, which directly contributes to the acceleration of data access (Liu, 2024).

On the other hand, the Local-First model prioritizes data availability and performance by ensuring that data is stored on the local device first. This strategy minimizes the reliance on an internet connection, while improving the performance of local applications, especially those that require real-time data access. By focusing storage on the local device, this model significantly reduces latency, making it an ideal choice for applications that are sensitive to response time. While the hybrid model offers flexibility and cost efficiency, the Local-First model is superior in use cases that require high availability and low latency. Therefore, choosing between the two models largely depends on the specific needs of the application and the users being served.

CONCLUSION

In a highly dynamic digital era, decisions about data storage cannot only depend on the physical location of the data, but must be based on a comprehensive risk management approach. This study shows that both cloud storage and local storage have their own strengths and weaknesses in terms of security, data control, performance, scalability, and cost. Cloud storage excels in scalability and accessibility, but faces serious challenges related to privacy and data control. Meanwhile, local storage provides full control over data, but is limited in terms of flexibility and scalability. The most promising solution is the implementation of a hybrid model or local-first architecture that is able to combine the advantages of both. Technology companies are advised to implement a risk-based storage strategy by integrating proactive cybersecurity policies, strict access control, and redundancy and encryption as security standards. Thus, data security can be maintained without sacrificing the efficiency and flexibility of the company's information system

REFERENCES

Aguru, A., Mahadevan, R., Babu, E., Kaluri, R., Bashir, A., & Gadekallu, T. (2024). Scs: a secure cloud storage framework with enhanced integrity and auditability using consortium blockchain system.. https://doi.org/10.21203/rs.3.rs-3926696/v1

Alizadeh, H. and Karimpour, J. (2014). Analysis of quality of service in cloud storage systems. International Journal in Foundations of Computer Science & Technology, 4(6), 71-77. https://doi.org/10.5121/ijfcst.2014.4607

Alotaibi, S., Alomair, H., & Elhussein, M. (2019). Comparing Performance of Commercial Cloud Storage Systems: The Case of Dropbox and One Drive. International Conference on Computer and Information Sciences, 1–5. https://doi.org/10.1109/ICCISCI.2019.8716385

Anggraeni, SF (2018). POLEMIC OF PERSONAL DATA OWNERSHIP REGULATION: URGENCY FOR HARMONIZATION AND LEGAL REFORM IN INDONESIA. Journal of Law & Development, 48(4), 814. https://doi.org/10.21143/jhp.vol48.no4.1804

Asaad, R.R., & Saeed, V.A. (2022). A Cyber Security Threats, Vulnerabilities, Challenges and Proposed Solutions. Applied Computing Journal, 227. https://doi.org/10.52098/acj.202260

Asniar, A., & Sari, SK (2015). Utilization of Cloud Computing for Enterprise Resources Planning in Indonesia. INFOTEL JOURNAL, 7(1), 75. https://doi.org/10.20895/infotel.v7i1.33

Assyakurrohim, D., Ikhram, D., Sirodj, RA, & Afgani, MW (2022). Case Study Method in Qualitative Research. Journal of Science and Computer Education, 3(1), 1. https://doi.org/10.47709/jpsk.v3i01.1951

Author1, & Author2. (20 CE). Article Title.

Aziz, K. and Mahmood, B. (2022). Assured data deletion in cloud computing: security analysis and requirements. Indonesian Journal of Electrical Engineering and Computer Science, 28(2), 1174. https://doi.org/10.11591/ijeecs.v28.i2.pp1174-1183

Brilliana, FW (2022). Analysis of the Implementation of the Judicial Commission's Authority in Wiretapping Reviewed from the Concept of Al-Ḍararu Yuzālu Biqodri Al-Imkān. Journal of Indonesian Comparative of Syari Ah Law, 5(2), 187. https://doi.org/10.21111/jicl.v5i2.7684

Building a Fast and Efficient LSM-tree Store by Integrating Local Storage with Cloud Storage. (2022). ACM Transactions on Architecture and Code Optimization, 19(3), 1–26. https://doi.org/10.1145/3527452

Chintia, E., Nadiah, R., Ramadhani, HN, Haedar, ZF, Febriansyah, A., & Kom, M. (2019). The Most Common Cybercrime Cases in Indonesia and Their Handling. Journal of Information Engineering and Educational Technology, 2(2), 65. https://doi.org/10.26740/jieet.v2n2.p65-69

Commey, D., Griffith, S., & Dzisi, J. (2020). Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage. International Journal of Computer Applications, 177(40), 17. https://doi.org/10.5120/ijca2020919897

Daher, Z., & Hajjdiab, H. (2018). Cloud Storage Comparative Analysis Amazon Simple Storage vs. Microsoft Azure Blob Storage. International Journal of Machine Learning and Computing, 8(1), 85–89. https://doi.org/10.18178/IJMLC.2018.8.1.668

Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S.U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, 15(11), 1981. https://doi.org/10.3390/sym15111981

El-Booz, S., Attiya, G., & El-Fishawy, N. (2016). A secure cloud storage system combining time-based one-time password and automatic blocker protocol. Eurasip Journal on Information Security, 2016(1). https://doi.org/10.1186/s13635-016-0037-0

Eyers, D., Routray, R., Zhang, R., Willcocks, D., & Pietzuch, P. (2011). Configuring large-scale storage using a middleware with machine learning. Concurrency and Computation Practice and Experience, 23(17), 2063-2077. https://doi.org/10.1002/cpe.1716

Fauziah, IS, & Apriani, R. (2021). Legal Review of Protection of Banking Customers Using Internet Banking Services. Face of Law, 5(2), 500. https://doi.org/10.33087/wjh.v5i2.557

Feng, Q., Han, J., Gao, Y., & Meng, D. (2012). Magicube: high reliability and low redundancy storage architecture for cloud computing.. https://doi.org/10.1109/nas.2012.15

Gao, G., Fei, H., & Qin, Z. (2020). An efficient certificateless public auditing scheme in cloud storage. Concurrency and Computation Practice and Experience, 32(24). https://doi.org/10.1002/cpe.5924

Gavali, V. N., More, R. P., & Potdukhe, S. D. (2014). A Review on Cloud Storage Performance to Improve File Accessing Efficiency. International Journal of Engineering Research and Technology, 3(11). https://www.ijert.org/research/a-review-on-cloud-storage-performance-to-improve-file-accessing-efficiency-IJERTV3IS110745.pdf

Goncalves, G., Vieira, A. B., & Almeida, J. M. (2018). On the Cost-Benefit Tradeoffs of Cloud Storage Services for End Users and Service Providers. https://doi.org/10.5753/SBRC_ESTENDIDO.2018.14186

Gudimetla, S. (2024). Data encryption in cloud storage. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets50637

Haoran, W., Tong, W., Gao, Q., & Zheng, S. (2015). A data deduplication method in the cloud storage based on fp-tree., 557-562. https://doi.org/10.1109/iccsnt.2015.7490809

Haryani, P., Ariyana, R. Y., Majid, I. A., & Susanto, Fx. G. P. (2024). Comparative Analysis of Nextcloud and Owncloud Performance as Infrastructure as a Service (IaaS) Based Cloud Storage. Compiler, 13(2), 73. https://doi.org/10.28989/compiler.v13i2.2667

Heo, H., Ahn, C., & Kim, D. (2016). Parity data de-duplication in all flash array-based openstack cloud block storage. Ieice Transactions on Information and Systems, E99.D(5), 1384-1387. https://doi.org/10.1587/transinf.2016edl8006

Herdiana, Y., Munawar, Z., & Putri, NI (2021). Mitigating Cybersecurity Risk Threats During the Covid-19 Pandemic. Journal of ICT Information Communication & Technology, 20(1), 42. https://doi.org/10.36054/jict-ikmi.v20i1.305

Huang, P., Fan, K., Yang, H., Zhang, K., Li, H., & Yang, Y. (2020). A collaborative auditing blockchain for trustworthy data integrity in cloud storage system. Ieee Access, 8, 94780-94794. https://doi.org/10.1109/access.2020.2993606

I. Samy, O. O. Koyluoglu and A. S. Rawat, "Efficient data access in hybrid cloud storage," 2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2017, pp. 1-8, doi: 10.1109/ALLERTON.2017.8262711. keywords: {Cloud computing;Maintenance engineering;Bandwidth;Encoding;Business;Servers;Electronic mail},

Idellie, PL, & Atok, RM (2023). Cyber Loss Distribution Modeling with Copula Approach and Cyber Insurance Premium Calculation. ITS Science and Arts Journal, 12(1). https://doi.org/10.12962/j23373520.v12i1.97479

J. E, Y. Cui, M. Ruan, Z. Li and E. Zhai, "HyCloud: Tweaking Hybrid Cloud Storage Services for Cost-Efficient Filesystem Hosting," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019, pp. 2341-2349, doi: 10.1109/INFOCOM.2019.8737399. keywords: {Cloud computing;Data transfer;Relays;Encoding;Computer science;Benchmark testing;Metadata},

Jeevitha, B. K., Thriveni, J., & Venugopal, K. R. (2016). Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey. International Journal of Computer Applications, 156(12), 16. https://doi.org/10.5120/ijca2016912513

Jiang, G. and Zhang, Q. (2017). Adaptive multi-copy layout algorithm based on mass storage system. Advances in Modelling and Analysis B, 60(2), 469-492. https://doi.org/10.18280/ama_b.600215

Kanatt, S., Talwar, P., & Jadhav, A. (2020). Review of Secure File Storage on Cloud using Hybrid Cryptography. International Journal of Engineering Research And, 2. https://doi.org/10.17577/ijertv9is020014

Kang, S., Veeravalli, B., Aung, K., & Jin, C. (2014). An efficient scheme to ensure data availability for a cloud service provider., 15-20. https://doi.org/10.1109/bigdata.2014.7004378

Kanumuri, S. (2024). Cloud Storage Cost Optimization: Advanced Techniques and Case Studies. https://doi.org/10.47363/jaicc/2024(3)250

Kulkarni, G., Waghmare, R., Palwe, R., Waykule, V., Bankar, H., & Koli, K. (2012). Cloud storage architecture. 76. https://doi.org/10.1109/tssa.2012.6366026

Kumar, M. and Nagalakshmi, P. (2019). Security issues of cloud computing - a survey. International Journal of Research in Advent Technology, 7(5), 316-322. https://doi.org/10.32622/ijrat.752019108

Latifah, E., & Abdullah, R. (2024). PRINCIPLES OF ISLAMIC ECONOMICS IN SHARIA FINANCIAL MANAGEMENT. Journal of International Development Economics., 2(2), 98. https://doi.org/10.62668/jide.v2i02.1186

Li, W., Yang, Y., & Yuan, D. (2016). Ensuring cloud data reliability with minimum replication by proactive replica checking. Ieee Transactions on Computers, 65(5), 1494-1506. https://doi.org/10.1109/tc.2015.2451644

Li, Y., Guo, K., Wang, X., Soljanin, E., & Woo, T. (2015). Sears: space efficient and reliable storage system in the cloud.. https://doi.org/10.1109/lcn.2015.7366342

Liu, Hongtao. (2024). Optimization and performance improvement of distributed data storage in hybrid storage systems. World Journal of Advanced Engineering Technology and Sciences, 2024, 13(01), 459–467. 10.30574/wjaets.2024.13.1.0443.

Mahendar, A. and Chatrapati, K. (2015). Mutual trust to provide data security in cloud computing and outsourced databases. Journal of Technological Advances and Scientific Research, 1(2), 75-82. https://doi.org/10.14260/jtasr/2015/10

Malaiyappan, J. N. A., Shanmugam, L., Thirunavukkarasu, K., & Mohamed, I. A. (2024). Scalable Distributed Storage Systems: Comparative Study of Key Technologies. International Journal For Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2024.v06i02.16338

Mandava, L. and Xing, L. (2017). Reliability analysis of cloud-raid 6 with imperfect fault coverage. IJPE. https://doi.org/10.23940/ijpe.17.03.p5.289297

Niu, X. (2017). Fine-grained access control scheme based on cloud storage., 512-515. https://doi.org/10.1109/iccnea.2017.48

O'Neill, V. and Soh, B. (2023). Spot market cloud orchestration using task-based redundancy and dynamic costing. Future Internet, 15(9), 288. https://doi.org/10.3390/fi15090288

Paryati, P. (2015). INFORMATION SYSTEM SECURITY. National Informatics Seminar (SEMNASIF), 1(4). http://jurnal.upnyk.ac.id/index.php/semnasif/article/download/743/621

Peng, J. (2014). A new model of data protection on cloud storage. Journal of Networks, 9(3). https://doi.org/10.4304/jnw.9.3.666-671

Pratiwi, AOS, & Sari, NR (2019). ABOVE THERAPY: GUIDANCE AND COUNSELING SERVICE SOLUTION TO PREVENT DELINQUENT BEHAVIOR IN ISLAMIC HIGH SCHOOL STUDENTS. AR-RAHMAN GUIDANCE AND COUNSELING JOURNAL, 5(1), 55. https://doi.org/10.31602/jbkr.v5i1.1840

Rahman, I., Sahrul, S., Mayasari, RE, Nurapriyanti, T., & Yuliana, Y. (2023). Consumer Protection Law in the E-Commerce Era: Navigating Consumer Protection Challenges in the Digital Trading Environment. Journal of Law and Human Rights Wara Sains, 2(8), 704. https://doi.org/10.58812/jhhws.v2i08.605

Rodrigues, J., Ferreira, B., & Domingos, H. (2013). Tms., 1-6. https://doi.org/10.1145/2541608.2541610

Rutania, Y., & Ganggi, RIP (2021). Personal Information Management Behavior of Digital Documents of Lectures in Library Science Students at Diponegoro University. Anuva Journal of Library and Information Culture Studies, 5(2), 199. https://doi.org/10.14710/anuva.5.2.199-212

Saputra, LA, Akbar, FM, Cahyaningtias, F., Ningrum, MP, & Fauzi, A. (2023). Security Threats to Corporate Management Information Systems. Nusantara Cyber Education Journal, 1(2), 58. https://doi.org/10.38035/jpsn.v1i2.48

Setiawan, MCA, Ginting, GKN, & Ilmar, A. (2020). The Relationship Between Identity Politics and Trade Protectionism under the Donald Trump Administration. Journal of Political Issues, 2(1), 58. https://doi.org/10.33019/jpi.v2i1.32

Sheela, M. (2022). Robust key revelation of public auditing prototype for secure cloud storage. Interantional Journal of Scientific Research in Engineering and Management, 06(02). https://doi.org/10.55041/ijsrem11717

Shengbin, W. (2020). Analysis of Big Data Cloud Storage Technology Based on Information Fusion Technology. https://doi.org/10.23977/iccia2020050

Shi, Y. (2018). Data Security and Privacy Protection Data Security and Privacy Protection in Public Cloud. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1812.05745

Shyamala, D. and S., F. (2015). Enhanced intensive indexing (i2d) de-duplication for space optimization in private cloud storage backup. International Journal of Computer Theory and Engineering, 7(2), 113-119. https://doi.org/10.7763/ijcte.2015.v7.941

Song, L., Wang, T., Zhang, L., & Song, X. (2015). Research and application of redundant data deleting algorithm based on the cloud storage platform. The Open Cybernetics & Systemics Journal, 9(1), 50-54. https://doi.org/10.2174/1874110x01509010050

Sreeramulu, M.D., (2024). Analysis of cloud computing and cloud storage in mobile forensics using the dematel method. cset, 2(2), 33-43. https://doi.org/10.46632/cset/2/2/4

Tudoran, R., Costan, A., & Antoniu, G. (2013). Datasteward: using dedicated compute nodes for scalable data management on public clouds.. https://doi.org/10.1109/trustcom.2013.129

Umar, R., Riadi, I., & Handoyo, E. (2019). Information System Security Analysis Based on COBIT 5 Framework Using Capability Maturity Model Integration (CMMI). JOURNAL OF BUSINESS INFORMATION SYSTEMS, 9(1), 47. https://doi.org/10.21456/vol9iss1pp47-54

Vimal, V. (2019). An efficient and secure query processing and indexing model for secure dynamic cloud storage. Turkish Journal of Computer and Mathematics Education (Turcomat), 10(2), 1043-1048. https://doi.org/10.17762/turcomat.v10i2.13623

Wu, J., Li, Y., Wang, T., & Ding, Y. (2019). Cpda: a confidentiality-preserving deduplication cloud storage with public cloud auditing. Ieee Access, 7, 160482-160497. https://doi.org/10.1109/access.2019.2950750

Xu, H. and Bhalerao, D. (2015). Reliable and secure distributed cloud data storage using reed-solomon codes. International Journal of Software Engineering and Knowledge Engineering, 25(09n10), 1611-1632. https://doi.org/10.1142/s0218194015400355

Xu, P., Zhao, N., Wan, J., Liu, W., Chen, S., Zhou, Y., … & Tan, Z. (2022). Building a fast and efficient lsm-tree store by integrating local storage with cloud storage. Acm Transactions on Architecture and Code Optimization, 19(3), 1-26. https://doi.org/10.1145/3527452

Xu, P., Zhao, N., Wan, J., Liu, W., Chen, S., Zhou, Y., … & Xie, C. (2021). Building a fast and efficient lsm-tree store by integrating local storage with cloud storage., 125-134. https://doi.org/10.1109/cluster48925.2021.00032

Yahya, F., Chang, V., Walters, R., & Wills, G. (2019). A security framework to protect data in cloud storage.. https://doi.org/10.5220/0007737603070314

Yang, C., Liu, Y., Tao, X., & Zhao, F. (2020). Publicly verifiable and efficient fine-grained data deletion scheme in cloud computing. Ieee Access, 8, 99393-99403. https://doi.org/10.1109/access.2020.2997351

Yang, C., Tao, X., & Zhao, F. (2019). Publicly verifiable data transfer and deletion scheme for cloud storage. International Journal of Distributed Sensor Networks, 15(10), 155014771987899. https://doi.org/10.1177/1550147719878999

Yang, S., Hareedy, A., Calderbank, R., & Dolecek, L. (2019). Hierarchical coding to enable scalability and flexibility in heterogeneous cloud storage.. https://doi.org/10.1109/globecom38437.2019.9014049

Yu, H., Cai, Y., & Kong, S. (2016). An efficient public auditing scheme for cloud storage server.. https://doi.org/10.2991/aest-16.2016.97

Zeng, W. and Zhao, Y. (2013). Mobile storage and data security management research. Applied Mechanics and Materials, 325-326, 1661-1664. https://doi.org/10.4028/www.scientific.net/amm.325-326.1661

Zhang, F., Xu, J., & Yang, G. (2023). Design of regenerating code based on security level in cloud storage system. Electronics, 12(11), 2423. https://doi.org/10.3390/electronics12112423

Zhang, G., Bao, W., Zhu, X., Zhao, W., & Yan, H. (2018). A server consolidation method with integrated deep learning predictor in local storage based clouds. Concurrency and Computation Practice and Experience, 30(23). https://doi.org/10.1002/cpe.4503

Zhang, W., Ma, C., Sha, W., & Zhou, Q. (2015). Research of data security in cloud storage.. https://doi.org/10.2991/iiicec-15.2015.192

Zhu, B., Shum, K., Li, H., & Hou, H. (2014). General fractional repetition codes for distributed storage systems. Ieee Communications Letters, 18(4), 660-663. https://doi.org/10.1109/lcomm.2014.030114.132694

Ács, S., Gergely, M., Kacsuk, P., & Kozlovszky, M. (2013). Block level storage support for open source iaas clouds., 262-268. https://doi.org/10.1109/pdp.2013.45