Review article / Pregledni rad

MIGRATING DATA TO THE CLOUD: AN ANALYSIS OF CLOUD STORAGE PRIVACY AND SECURITY ISSUES AND SOLUTIONS

MARIJA KUŠTELEGA
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
marija.kustelega@foi.unizg.hr

RENATA MEKOVEC
University of Zagreb
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
renata.mekovec@foi.unizg.hr

ABSTRACT

The rise of a digital economy has transformed how individuals do business and carry out daily tasks, including how data is maintained. Because of the vast amount of data that organizations own, cloud storage, a component of the cloud computing paradigm, has emerged as a feasible solution to many businesses' data storage concerns. Despite this, organizations are still cautious about moving all of their data to the cloud due to security concerns, particularly since data management is outsourced to third parties. The aim of this paper is to provide an overview of current challenges in the field of cloud storage privacy and security, with an emphasis on issues related to data confidentiality, integrity, and availability. Using a comprehensive literature study, this research investigates innovative strategies for creating a secure cloud storage environment. The idea of maintaining privacy and data security through the very design of the services, or through the so-called "privacy by design" approach, is explained while avoiding getting into the technical details of how the algorithms and presented solutions work.

KEYWORDS: digital economy, cloud, storage, privacy, security, challenges, solutions

1. INTRODUCTION

The Digital Economy Report 2021 provides insight into the development and policy implications of cross-border digital data flows, focusing on rapidly expanding digital technologies, which have become a vital resource for today's economy [United Nations Conference on Trade and Development (UNCTAD), 2021]. Cloud computing is listed in the report as one of the critical fuels of the digital economy, particularly regarding the expansion of the cloud market. A 2019 survey of 400 professionals from industries worldwide revealed 84% used the cloud for data storage or backup, while 5% planned to implement it within the next six months [Statista, 2022]. With the increasing use of cloud technology across various industries, migrating data to the cloud poses significant privacy and security challenges.

1.1. DIGITAL ECONOMY AND CLOUD COMPUTING

The digital economy has shifted from goods and services to information production, thereby enabling new ways of creating value [UNCTAD, 2019]. As a result, this data-driven economy emerges due to the benefits it offers for strategic trade [Ciuriak, 2020].

The digital economy consists of three main components [UNCTAD, 2019]:

- core aspects (digital infrastructure and hardware),
- digital and information technology sectors (digital platforms, payments etc.),
- and the broader idea of digitized sectors (places where digital goods and services are primarily used, like finance, tourism, and transport).

The cloud computing paradigm has become an important aspect of the growing digital economy due to its tight link to technology stated in all three components. The National Institute of Standards and Technology (NIST) describes cloud computing as a concept for on-demand network access to shared computer resources, including cloud storage, as one example of these resources [Mell and Grance, 2011].

Consideration for the legal obligations should be analyzed when storing data. In Article 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), data processing principles such as the storage of personal data and measures to prevent unlawful processing are outlined. In order to promote data sharing among enterprises, the European Union (EU) enacted the Data Governance Act (DGA) and is drafting the Data Act proposal; nevertheless, these regulations may compromise data privacy under the GDPR [Eur-lex.com, 2022]. Moreover, it is important to mention the Free Flow of Non-Personal Data Regulation, which enabled non-personal data storage, processing, and transfer, as well as the development of Switching Cloud Providers and Porting Data (SWIPO) codes of conduct for enforcing data portability across cloud providers [Eur-lex.com, 2022]. Additionally, one of the Data Act proposal's specific goals deals with problem of simplifying cloud and edge service switching, enabling organizations to move data and assets between providers to build trust and facilitate data sharing [Eur-lex.com, 2022]. These principles are crucial for the further development of the digital economy.

1.2. CIA triad

According to the NIST: "Information system-related security risks arise from the loss of confidentiality, integrity, or availability of information or information systems" [Chandramouli and Pinhas, 2020]. The CIA triad, a commonly used framework for identifying security risks, stands for [Fortinet, n.d.]:

- **C**onfidentiality: keeping data hidden or private from unauthorized users,
- **I**ntegrity: ensuring accurate and dependable data that has not been altered,
- **A**vailability: proper and on-time functioning of systems and applications.

NIST security recommendations for storage infrastructures include data protection using encryption, regular backup testing to verify integrity, and multiple authentication servers to ensure availability [Chandramouli and Pinhas, 2020]. In this regard, Article 32 of GDPR [L

119/1] outlines technical and organizational measures for ensuring the CIA triad, including pseudonymization, encryption, regular testing, and evaluation.

The aim of this paper is to provide an overview of current challenges in the field of cloud storage privacy and security, focusing on issues related to data confidentiality, integrity, and availability. The following research questions (RQs) were developed to achieve this goal:

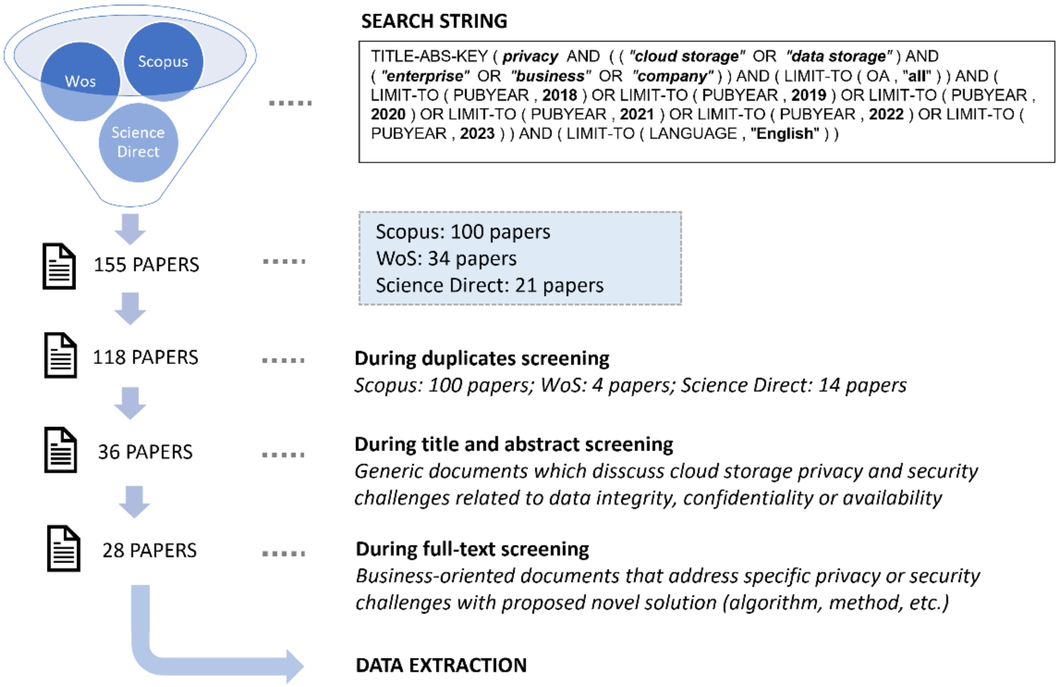
- RQ1: What are the key challenges with cloud storage privacy and security issues related to data confidentiality, integrity, and availability?
- RQ2: What modern solutions are being developed for data storage security and privacy protection in the cloud?

The remainder of the paper is structured as follows: Section 2 addresses applied research methodology; Section 3 presents results and findings; Section 4 discusses main challenges; Section 5 presents literature solutions; and Section 6 concludes the research article.

2. METHODOLOGY

The literature review was conducted utilizing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology, divided into search, screening, and data extraction phases [Moher et al., 2009]. Within the search phase, the appropriate search string was used to discover relevant publications on privacy and cloud data storage for business purposes. Scopus, WoS, and Science Direct databases were searched for articles that satisfied search criteria, limited to English-language publications published in the last five years, beginning in 2018 and ending in July 2023. Figure 1 presents the PRISMA methodology's steps graphically and provides thorough explanations.

Figure 1. PRISMA diagram with results of the literature search and screening



TITLE-ABS-KEY (***privacy*** AND ((***"cloud storage"*** OR ***"data storage"***) AND (***"enterprise"*** OR ***"business"*** OR ***"company"***)) AND (LIMIT-TO (OA , **"all"**)) AND (LIMIT-TO (PUBYEAR , **2018**) OR LIMIT-TO (PUBYEAR , **2019**) OR LIMIT-TO (PUBYEAR , **2020**) OR LIMIT-TO (PUBYEAR , **2021**) OR LIMIT-TO (PUBYEAR , **2022**) OR LIMIT-TO (PUBYEAR , **2023**)) AND (LIMIT-TO (LANGUAGE , **"English"**))

Scopus: 100 papers
WoS: 34 papers
Science Direct: 21 papers

During duplicates screening
Scopus: 100 papers; WoS: 4 papers; Science Direct: 14 papers

During title and abstract screening
Generic documents which disscuss cloud storage privacy and security challenges related to data integrity, confidentiality or availability

During full-text screening
Business-oriented documents that address specific privacy or security challenges with proposed novel solution (algorithm, method, etc.)

Source: Authors

The articles were analyzed by duplicate screening, title and abstract screening, and full-text screening. Inclusion and exclusion criteria were used to narrow the pool of articles. Articles had to address cloud storage challenges and at least one of the CIA triad issues to be included for further analysis. The analysis excluded studies that did not meet the search criteria or referred to articles with systematic literature reviews without presenting their own solution. Articles that met the inclusion and exclusion criteria were extracted and analyzed.

3. RESULTS

This study examined 28 papers to provide a systematic review of challenges and solutions associated with cloud storage over the last five years. The results were processed in the following order: identification of challenges, categorization of challenges, and presentation of solutions. Firstly, cloud storage issues were identified using the CIA triad. Table 1 depicts an overview of the main challenges mapped into the CIA triangle, where "C" refers to confidentiality, "I" to integrity, and "A" to data availability issues. If the security issues were addressed in publications, they were labeled with "x"; otherwise, the cells were left blank.

Table 1. Identification of challenges

No	Author(s)	Main challenges	C	I	A
1.	Liu et al. (2022)	Protect highly sensitive data during public sharing.	x	x	
2.	Chen et al. (2022)	Protect data shared between enterprises.	x	x	
3.	Vo et al. (2021)	Protect database and enable encrypted keyword search.	x		
4.	Rauthan & Vaisla (2021)	Ensure user data confidentiality with robust database.	x		
5.	Khashan (2020)	Secure outsourced and shared cloud data.	x	x	
6.	Li et al. (2019)	Protect smart grid data and enable keyword search.	x		
7.	Miao et al. (2018)	Support multi-keyword search and result verification.	x	x	
8.	Li et al. (2020)	Ensure data integrity scheme with quantum security.		x	
9.	Challagidad & Birje (2020)	Provide multi-authority access control for user data.	x	x	
10.	Kumar & Shafi (2020)	Protect stored data with RSA public key cryptosystem.	x	x	
11.	KL & Nair (2019)	Secure locking system for critical data.	x	x	x
12.	Yadav et al. (2019)	Provide reliable system for monitoring cloud data.	x	x	
13.	Liang et al. (2018)	Secure sharing and collaboration in healthcare systems.	x	x	x
14.	Mohammed & Abed (2020)	Secure storage of cloud data at rest.	x		
15.	Berrima et al. (2018)	Ensure data privacy and user authentication.	x		
16.	Yan et al. (2021)	Safeguard uploader privacy in group-shared data.	x	x	
17.	Divya et al. (2019)	Protect storage and enable keyword data retrieval.	x	x	
18.	Wu et al. (2019)	Enable privacy and retrieval in pay-as-you-go model.	x	x	
19.	Pinheiro et al. (2018)	Build security architecture for cloud data monitoring.	x	x	x
20.	Zheng et al. (2022)	Provide access control for user attribute revocation.	x		
21.	Bian et al. (2022)	Safeguard sensitive data during audits.	x	x	
22.	Uddin et al. (2021)	Prevent cloud threats in virtualization platforms.	x	x	x
23.	Jl & Maria (2020)	Improve data integrity in dynamic cloud auditing.	x	x	
24.	Nithya & Rhymend Uthariaraj (2021)	Preserve data integrity and key-exposure in multiple cloud storage.	x	x	
25.	Almuzaini et al. (2022)	Improve key aggregate cryptosystem for health systems.	x	x	
26.	Zhang et al. (2020)	Ensure cloud audit protocol with group user privacy.	x	x	
27.	Tian & Wang (2020)	Ensure secure deletion of sensitive data.	x	x	
28.	Zhang et al. (2019)	Enhance privacy of Internet of Things (IoT) layers.	x	x	x

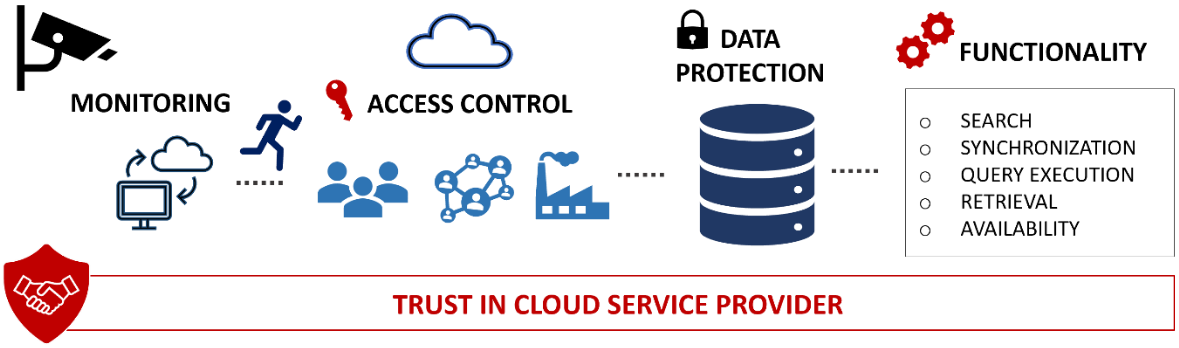
Source: Authors

The results showed that various industries have taken cloud security challenges into account. Most articles emphasized data integrity and confidentiality, with less focus on data availability issues. Further findings will be discussed in the sections that follow where first the categorization of privacy and security challenges is presented and then proposed solutions.

4. CATEGORIZATION OF PRIVACY AND SECURITY CHALLENGES

Companies often use multiple cloud storage to reduce costs and prevent vendor lock-in [Nithya & Rhymend Uthariaraj, 2021], but this requires security measures to protect sensitive data [KL and Nair, 2019]. This is particularly important for hospitals, banks, and IoT devices, which require verified data integrity for proper data analysis [Jl & Maria, 2020]. Based on a literature review, the recognized privacy and security challenges can be divided into four primary categories: monitoring, access control, data protection, and functionality challenges. In order to better visualize the main challenges, their graphic representation is shown in Figure 2.

Figure 2. Categorization of challenges



Source: Authors

According to this, all challenges can be connected to the larger problem of trust in service providers. Concerns related to monitoring, access control and data protection directly impact security and privacy. Despite not immediately jeopardizing safe storage, functional issues are identified as one of the obstacles to overcome when developing cloud storage systems.

4.1. MONITORING

Cloud service providers monitor and maintain a wide range of services for end users and businesses, making it challenging to track all cloud activities and perform efficient data security monitoring [Yadav et al., 2019]. Cloud service providers may seek for sensitive customer information during data integrity audits [Bian et al., 2022], return incorrect or irrelevant search results [Miao et al., 2018] or can easily fake authenticator to provide false proof of integrity [Zhang et al., 2020]. Data leakage may also occur when providers fail to destroy every copy of erased data, so users must be sure that they will delete all backups [Tian & Wang, 2020]. Sensitive data necessitates stronger privacy protection, but knowing when to do rigorous or less demanding checks remains difficult. It would be convenient if the user could choose when to execute further data integrity checks in the event of any security concerns. [Yadav et al., 2019]. According to Pinheiro et al. (2018), the security architecture must adjust the frequency of integrity checks based on the amount of trust in the cloud service provider. They underline the significance of observing cloud activities and proposing dynamic integrity checks with respect to the learned service provider behavior. Attacks are another thing to keep an eye on because they cause severe problems. Authors have addressed challenges with various attacks, such as inference attack [Vo et al., 2021], quantum attack [Li et al., 2020], side-channel attacks [Li et al., 2019], and keyword guessing attack [Miao et al., 2018]. In virtualized cloud infrastructure is common the "velocity-of-attack", where security threats spread and escalate faster due to the expanded infrastructure [Uddin et al., 2021]. Jl & Maria (2020) highlighted the problem of launching a distributed denial-of-service (DDOS) attack, causing network congestion and degrading service quality. With a detailed study of a chosen protocol, Berrima et al. (2018) revealed an unidentified attack that endangers user privacy. Therefore, with continuous observation, it's possible to uncover previously hidden drawbacks and improve security. Furthermore, design systems should continuously monitor data and alert about potential attacks for ensuring storage security [Yadav et al., 2019].

4.2. ACCESS CONTROL

Due to the on-demand nature of cloud computing, it is essential to put strong security measures to regulate data access and prevent unauthorized access [Mohammed & Abed, 2020]. This applies to data transfer, where reliable verification and access control mechanisms need to be established [Almuzaini et al., 2022] and for better control of sensitive data, such as private medical data [Liang et al., 2018]. To ensure that vital data is safely kept in the cloud, it is crucial that only the authenticated user can access or download data [KL and Nair, 2019], so access structures should restrict data to only those users with matching attributes [Tian & Wang, 2020]. Furthermore, KL and Nair (2019) considered multi-authentication challenges with acceptable data availability, while Liang et al. (2018) explored blockchain and smart contracts for reliable data access when dealing with multiple users. Zheng et al. (2022) focused on cloud access control in sensor networks and vehicular ad hoc networks (VANET). Considering cost effectiveness, systems with verifier authentication, may demand storage of verifier's unique key pairs, resulting in higher storage costs [Bian et al., 2022]. Moreover, cloud service providers face challenges in authenticating users while maintaining privacy. For instance, enterprise cloud storage systems with multiple user roles can compromise employee privacy through group user-based auditing protocols [Zhang et al., 2020]. To protect their employees' private data, organizations must provide fine-grained access control [Challagidad & Birje, 2020]. Berrima et al. (2018) analyzed private access control protocols where authenticate users must confirm storage rights without revealing their identity.

4.3. DATA PROTECTION

Data security was acknowledged in the new NIST Framework 2.0 draft as one of the outcomes to achieve in the prevention phase, distinguishing between securing data at rest, in use, and in transit [National Institute of Standards and Technology, 2023]. Rarely used archived documents pose a challenge due to poor access, allowing them to be compromised without the owner's knowledge. Mohammed and Abed (2020) focused on securing cloud data at rest to prevent leaks, illegal access, and threats. This is crucial, especially in smart grid data, as records contain common keywords, making them vulnerable to attacks [Li et al., 2019]. In order to secure storage, Vo et al. (2021) researched padding strategies against inference attacks, such as monitoring cluster caches and setting timers before flushing. Smart grid data is unique in that it is often updated and typically contains a large number of attributes, demanding a safe search index for performing such alternations [Li et al., 2019]. Providing effective integrity checks in situations involving dynamic data operations is likewise highly difficult [Divya et al., 2019]. Cloud service providers can free up storage by deleting or hiding instances of data loss [Wu et al., 2019], but this presents challenges for companies handling massive amounts of data. To ensure proper data handling, cloud service providers should follow appropriate practices for information assurance [Uddin et al., 2021], including modification and removal procedures. Patients' medical records, according to Liu et al. (2022), can be useful data sources for both researchers and healthcare providers. Shared data involves collaboration among several people, so Zhang et al. (2019) tackle the challenge of developing secure key sharing schemes in IoT systems, while Liang et al. (2018) underlined the importance of secure communication channels for requesting personal healthcare or insurance services, as well as enabling effective collaboration between them. In addition to sharing publicly available data, it's equally important to protect privacy when sharing data within or between organizations. Chen et al. (2022) dealt with ensuring safe data transfer between approved businesses, while Yan et al. (2021) investigated the issue of preserving file uploaders' anonymity in internal data shared between workgroups.

4.4. FUNCTIONALITY

It is difficult to design a database structure that is both secure and efficient [Rauthan & Vaisla, 2021]. An encrypted database limits the ability to query parts [Li et al., 2019], thus making traditional query execution extremely challenging [Rauthan & Vaisla, 2021]. It disables search functionality important for searching data gathered by smart grid devices, such as metering data [Li et al., 2019]. Divya et al. (2019) explore a "coordinate matching" keyword search strategy to gather linked documents; Vo et al. (2021) explore a search secure against inference attacks; and Miao et al. (2018) dealt with multiple keyword searches. Wu et al. (2019) examine safeguarding user privacy while enabling functionality like data retrieval and audits suitable for public utility cloud services, such as electricity, where customers pay based on storage volume and duration. Lack of agreement among participants can lead to availability issues, such as bottlenecks causing system crashes [Uddin et al., 2021]. Research on safe transmission after cloud server failures [Zhang et al., 2019] and ensuring data availability [KL & Nair, 2019] can help address these issues.

5. PROPOSED TRENDS FOR ADDRESSING PRIVACY AND SECURITY CHALLENGES

The authors primarily used encryption and digital signatures in their solutions, combined with methods to preserve integrity. To guarantee data security, KL & Nair (2019) introduced the Data Storage Lock Algorithm (DSLA), Wu et al. (2019) designed a privacy-preserving proof of storage for the pay-as-you-go business model, while Mohammed and Abed (2020) developed an encryption framework to defend cloud data at rest. Privacy preservation methods include certificateless auditing [Bian et al., 2022], enhanced integrity methods [Jl & Maria, 2020], and forward secure public auditing scheme to prevent key exposure attacks [Li et al., 2020]. To maintain uploader anonymity in group-shared data, Yan et al. (2021) developed a certificateless public auditing protocol, while Zhang et al. (2020) designed a group user privacy auditing protocol to prevent cloud server's integrity falsification. Identity-based techniques include parallel key insulation [Nithya & Rhymend Uthariaraj, 2021] and sanitizable digital signatures [Liu et al., 2022]. Khashan (2020) introduced user-side encrypted file systems (OutFS) for secure data exchange, while Zhang et al. (2019) proposed compressed sensing fault-tolerant encryption for secure key sharing in IoT cloud systems. Some authors explored blockchain solutions for virtualization [Uddin et al., 2021], enterprise data sharing scheme [Chen et al., 2022], and a safe collaboration system for sharing health data [Liang et al., 2018]. A fine-grained data deletion system with attribute association (ADAA) was proposed by Tian & Wang (2020) for secure data deletion. For data control, Yadav et al. (2019) proposed a monitor-based scheme, while Pinheiro et al. (2018) established a security architecture and protocol that dynamically modify checks based on trust in the cloud service provider. In terms of ensuring access control across multiple authorities, Challagidad and Birje (2020) created a hierarchy access structure for privacy protection, Berrima et al. (2018) introduced a corrected private access control, and Zheng et al. (2022) introduced a user attribute revocation strategy. For functionality issues, Vo et al. (2021) proposed encrypted document database search, while Li et al. (2019) focused on searchable smart grid data. For data retrieval, Divya et al. (2019) developed cloud storage with trust manager, while Miao et al. (2018) proposed verifiable multi-keyword search. Rauthan & Vaisla (2021) developed solution for efficient query execution, Kumar & Shafi (2020) proposed a modified RSA public key cryptosystem, and Almuzaini et al. (2022) developed a scalable key aggregate cryptosystem for health data protection.

6. CONCLUSION

This study is important since it identifies challenges and solutions related to privacy and security protection when using cloud storage. Secure cloud data storage face with monitoring, access control, data protection, and functionality challenges, each requiring a distinct strategy. While static data needs robust measures for safe storage, dynamic data needs procedures to avoid unauthorized changes. Many of these challenges are linked to the broader issue of trust in cloud service providers, demanding constant data monitoring. Proposed solutions for secure cloud storage like encryption, signatures, data sanitization and integrity methods follow guidelines presented in the NIST framework. These findings can serve as a reminder of the security risks associated with cloud storage with the aim of encouraging the implementation of presented solutions. Further research is needed to determine whether the concept of privacy by design, which seeks to provide security and privacy while maintaining high service functionality, can really be implemented.

REFERENCES

[1] Almuzaini, K. K., Sinhal, A. K., Ranjan, R., Goel, V., Shrivastava, R., & Halifa, A. (2022). Key Aggregation Cryptosystem and Double Encryption Method for Cloud-Based Intelligent Machine Learning Techniques-Based Health Monitoring Systems. *Computational Intelligence and Neuroscience*, 2022.

[2] Berrima, M., Lafourcade, P., Giraud, M., & Rajeb, N. B. (2018). Formal analysis of a private access control protocol to a cloud storage. *International Journal of Innovative Computing and Applications*, 9(3), 150-164.

[3] Bian, G., Guo, X., Li, R., Qu, W., & Zhao, Y. (2022).Certificateless Data Integrity Auditing in Cloud Storage with a Designated Verifier and User Privacy Preservation. *Electronics*, 11(23), 3901.

[4] Challagidad, P. S., & Birje, M. N. (2020). Efficient multi-authority access control using attribute-based encryption in cloud storage. *Procedia Computer Science*, 167, 840-849.

[5] Chandramouli, R., Pinhas, D. (2020). Security Guidelines for Storage Infrastructure (No. NIST Special Publication (SP) 800-209).*National Institute of Standards and Technology*.

[6] Chen, C. L., Yang, J., Tsaur, W. J., Weng, W., Wu, C. M., & Wei, X. (2022). Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application. *Sensors*, 22(3), 1146.

[7] Ciuriak, D. (2020). Economic Rents and the Contours of Conflict in the Data-driven Economy. *Policy Brief, Centre for International Governance Innovation*, June.

[8] Divya, S. V., Shaji, R. S., & Venkadesh, P. (2019). A combined data storage with encryption and keyword based data retrieval using SCDS-TM model in cloud. *Malaysian Journal of Computer Science*, 32(3), 163-185.

[9] Eur-lex.com (2022). Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0068, downloaded: [August, 12th 2023]

[10] Fortinet (n.d.). CIA Triad, https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions. , downloaded: [August, 12th 2023]

[11] Jl, J. D., & Maria, C. (2020). Data integrity method for dynamic auditing in cloud environment. *Indian Journal of Computer Science and Engineering*, 11(6), 843-850.

[12] Khashan, O. A. (2020). Secure outsourcing and sharing of cloud data using a user-side encrypted file system. *IEEE Access*, 8, 210855-210867.

[13] KL, A., & Nair, T. R. (2019). Data storage lock algorithm with cryptographic techniques. *International Journal of Electrical & Computer Engineering (2088-8708)*, 9(5).

[14] Kumar, Y. K., & Shafi, R. M. (2020). An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem. *International Journal of Electrical and Computer Engineering*, 10(1), 530.

[15] L 119/1. n.d. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[16] Li, H., Liu, L., Lan, C., Wang, C., & Guo, H. (2020). Lattice-based privacy-preserving and forward-secure cloud storage public auditing scheme. *IEEE Access*, 8, 86797-86809.

[17] Li, J., Niu, X., & Sun, J. S. (2019). A practical searchable symmetric encryption scheme for smart grid data. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[18] Liang, X., Shetty, S., Tosh, D., Bowden, D., Njilla, L., Kamhoua, C. (2018). Towards blockchain empowered trusted and accountable data sharing and collaboration in mobile healthcare applications. *EAI Endorsed Transactions on Pervasive Health and Technology*, 4(15).

[19] Liu, Z., Ren, L., Li, R., Liu, Q., & Zhao, Y. (2022). ID-based sanitizable signature data integrity auditing scheme with privacy-preserving. *Computers & Security*, 121, 102858.

[20] Miao, Y., Ma, J., Liu, X., Liu, Z., Shen, L., & Wei, F. (2018). VMKDO: Verifiable multi-keyword search over encrypted cloud data for dynamic data-owner. *Peer-to-peer Networking and Applications*, 11, 287-297.

[21] Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology,* https://csrc.nist.gov/pubs/sp/800/145/final, downloaded: [August, 12th 2023]

[22] Mohammed, M., & Abed, F. (2020). A symmetric-based framework for securing cloud data at rest. *Turkish Journal of Electrical Engineering and Computer Sciences*, 28(1), 347-361.

[23] Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group*. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine, 151*(4), 264-269.

[24] National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD),

NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. https://doi.org/10.6028/NIST.CSWP.29.ipd

[25] Nithya, S. M. V., & Rhymend Uthariaraj, V. (2021). Identity-based Provable Data Possession for Multicloud Storage with Parallel Key-Insulation. *KSII Transactions on Internet and Information Systems (TIIS)*, 15(9), 3322-3347.

[26] Pinheiro, A., Dias Canedo, E., de Sousa Junior, R. T., de Oliveira Albuquerque, R., García Villalba, L. J., & Kim, T. H. (2018). Security architecture and protocol for trust verifications regarding the integrity of files stored in cloud services. *Sensors*, 18(3), 753.

[27] Rauthan, J. S., & Vaisla, K. S. (2021). Vrs-db: Preserve confidentiality of users' data using encryption approach. *Digital Communications and Networks*, 7(1), 62-71.

[28] Statista (2022). Cloud-based data storage or backup usage intentions in companies worldwide as of 2019, https://www.statista.com/statistics/1114013/worldwide-cloud-usage-for-data-storage-or-backup/#statisticContainer, downloaded: [June, 31th 2023]

[29] Tian, J., & Wang, Z. (2020). Fine-grained assured data deletion scheme based on attribute association. *Computers & Security*, 96, 101936.

[30] Uddin, M., Khalique, A., Jumani, A. K., Ullah, S. S., & Hussain, S. (2021). Next-generation blockchain-enabled virtualized cloud security solutions: review and open challenges. *Electronics*, 10(20), 2493.

[31] United Nations Conference on Trade and Development [UNCTAD] (2021). *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow*. United Nations publication. Sales No. E.21.II.D.18. New York and Geneva.

[32] United Nations Conference on Trade and Development [UNCTAD] (2019). *Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries*. United Nations publication. Sales No. E.19.II.D.17. New York and Geneva.

[33] Vo, V., Yuan, X., Sun, S., Liu, J. K., Nepal, S., & Wang, C. (2021). Shielddb: An encrypted document database with padding countermeasures. *IEEE Transactions on Knowledge and Data Engineering*.

[34] Wu, T., Yang, G., Mu, Y., Guo, F., & Deng, R. H. (2019). Privacy-preserving proof of storage for the pay-as-you-go business model. *IEEE Transactions on Dependable and Secure Computing*, 18(2), 563-575.

[35] Yadav, A. K., Ritika, M. L. G., & Garg, M. L. (2019). Monitoring Based Security Approach for Cloud Computing. *Ingénierie des Systèmes d Inf.,* 24(6), 611-617.

[36] Yan, H., Liu, Y., Zhang, Z., Wang, Q. (2021). Efficient privacy-preserving certificateless public auditing of data in cloud storage. *Security and Communication Networks*, 2021, 1-11.

[37] Zhang, J., Wang, B., Wang, X. A., Wang, H., & Xiao, S. (2020). New group user based privacy preserving cloud auditing protocol. *Future Generation Computer Systems*,106, 585-594.

[38] Zhang, P., Gao, J., Jia, W., & Li, X. (2019). Design of compressed sensing fault-tolerant encryption scheme for key sharing in IoT Multi-cloudy environment (s). *Journal of Information Security and Applications*, 47, 65-77.

[39] Zheng, F., Peng, X., & Li, Z. (2022). An efficient User's attribute revocation scheme suitable for data outsourcing in cloud storage. *Wireless Communications and Mobile Computing*, 2022.