ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 11, Issue 9, September 2024

A Survey on Privacy-Preserved Multi-Cloud Storage with Automated Security Bots

M.Dancily Jebamalar, Dr.J. Anthoniraj

Research Scholar, PG & Research Department of Computer Science, Jamal Mohamed College (Autonomous), (Affiliated to Bharathidasan University), Trichy – 620020.
Research Supervisor, Assistant Professor, Department of Computer Science, M.I.E.T Arts & Science College, Trichy – 620007.

ABSTRACT: In the era of computers, protecting personal information presents several difficulties, particularly in cloud storage settings where data security is crucial. Although cloud computing provides easily available storage options, it also exposes users to security risks. Many security flaws in the current cloud data storage methods make cost-effective and safe alternatives necessary. The usefulness of using multi-cloud storage strategies to overcome these obstacles is investigated in this survey. The suggested method maintains economic viability while improving security measures by utilizing several cloud providers. The system also incorporates defensive bots that are able to recognize and automatically counteract both external and internal attacks on data storage. These self-learning bots make sure that stored data is well protected by constantly changing to fend off new threats.

KEYWORDS: Privacy, Multi-Cloud Storage, Automated Security Bots, Data Security, Cloud Environments, Privacy Preservation

I. INTRODUCTION

The rise of data-driven technology in recent years has brought to light how crucial it is to maintain security and privacy in a number of industries, including data storage, parking, and healthcare. Data integrity and confidentiality have become critical as more and more businesses handle sensitive information via digital platforms. In order to overcome these obstacles, academics have looked at creative solutions that make use of developments in distributed computing, blockchain technology, and cryptography. The three noteworthy additions applied to the rapidly changing field of privacy-preserving technology. A privacy preserved recoverable encryption based on public and private blockchain is proposed by Du Ruizhong, Ma Caixia, and Li Mingyue. To meet the needs of contemporary data storage systems, a unique framework that makes use of blockchain technology improves the privacy and security of searchable encryption algorithms [1].

A secured and private parking guidance system employing localized differential privacy alongside elliptic curve cryptography. is introduced by Abdul Khaliq Awais and Anjum Adeel. The utilization of cryptographic methods and privacy-preserving protocols guarantees the confidentiality of user data while permitting customized suggestions. [2]. R. A. Khandaker Muhammad and Shakila Zaman investigate the use of Holochain for distributed security in IoT healthcare. Healthcare IoT solutions benefit from distributed ledger technology's ability to improve security and privacy. The suggested architecture provides strong security measures while preserving scalability and efficiency in the administration of healthcare data by utilizing the special qualities of Holochain. When taken as a whole, these works promote privacy-preserving technologies in a variety of fields and provide novel approaches to protect sensitive data in an increasingly interconnected digital environment [3].

II. LITERATURE SURVEY

Fahrianto Feri suggests using a dual-channel translation gateway to mediate IP to NDN. Using a double way translation gateway, this method—which is described in the publication—handles the switch from Internet Protocol (IP) to Named Data Networking (NDN). The suggested gateway makes it easier for IP and NDN networks to communicate with one another, which improves the efficiency and scalability of upcoming network designs through smooth integration and migration techniques [4]. Research on Big Data Privacy and Security Using copious Data Recovery methodologies and Data Obliviousness is presented by Funde Snehalata and Swain Gandharba [5]. Their recently released research delves into methods for protecting large data security and privacy using methods like data obliviousness and plentiful data recovery.

Organizations may ensure regulatory compliance and safeguard confidential data from unwanted access by utilizing these strategies to reduce privacy concerns and improve data security in large-scale data environments. Li Mingyue, Ha Guanxiong, Jia Chunfu, and Chen Hang look into a defense plan and threat model for channelized side attacks in client oriented de-duplication [6]. Their research on detecting and thwarting channeled attacks in client oriented de-duplication systems is described in depth in the paper. The researchers hope to protect the integrity and confidentiality of data stored in cloud settings by strengthening the security and resilience of de-duplication algorithms against possible attacks by putting up a complete defensive plan.

Contributions to Lightweight Data Possessed for Cloud Storage Using Indistinguishable concealment are made by Chaudhari Smita and Swain Gandharba. They examine methods for using indistinguishable obfuscation to achieve lightweight proven data possession in cloud storage systems in their most recent paper [7]. Through the use of this cryptographic primitive, the suggested method allows for effective and verifiable data possession proofs, improving cloud storage services' security and reliability while saving customers' computing costs.

Route oriented practical Content Caching along with Self Attentive in Hierarchical Federated Learning is introduced by Khanal Subina, Thar Kyi, and Huh Eui-Nam [8]. Their work on employing self-attention mechanisms to optimize content caching tactics in hierarchical federated learning environments was recently published in a journal. The suggested method improves data accessibility and lowers latency by proactively storing pertinent data along routing channels, which boosts federated learning systems' overall effectiveness and performance.

A Privacy Preserved Auditing with Secure Group Management is proposed by Kim Dongmin and Kim Kee Sung [9]. Their research, which is published in full, offers a private auditing plan with secure group management features for shared cloud data. The suggested approach ensures user privacy protection and accountability in cloud storage settings, while enabling efficient and safe auditing of shared data through the integration of cryptographic algorithms and access control mechanisms.

Multiple Keyword Ranking Search Encryption key for Data Shared in Cloud Computing is being investigated by Jinlu Liu and others [10]. Their study on how to enable multi-keyword ranked searchable encryption with wildcard keyword support in cloud computing settings was published in The Computer Journal. The suggested encryption approach improves data sharing capabilities while protecting user privacy and confidentiality in cloud-based data repositories by enabling effective and secure keyword-based search operations.

Research on linear group of Data Shared Cloud Assisted Industrial IOT is presented by T. Li, J. Zhang, Y. Shen, and J. Ma [11]. This allows industrial Internet of things (IIoT) systems that use cloud assistance to share data in a hierarchical and multi-group manner. The suggested strategy facilitates data-driven decision-making and optimization in industrial settings by enhancing cooperation and interoperability across varied IoT devices and apps through the establishment of effective data sharing channels.

Multi-user cloud-based Internet of Things applications, F. Rezaeibagha, Y. Mu, K. Huang, L. Chen, and L. Zhang provide Toward Secure Data Computation and Outsourcing [12]. Their research on methods for accomplishing safe data processing and outsourcing in multi-user cloud-based Internet of Things (IoT) environments was published in on Cloud Computing. The suggested method provides safe and effective data processing and outsourcing, guaranteeing data confidentiality and integrity in Internet of Things applications hosted on cloud platforms, by utilizing cryptographic primitives and secure computing protocols.

III. ADVANCEMENTS IN SECURE DATA SHARING AND ACCESS CONTROL MECHANISMS FOR DISTRIBUTED COMPUTING ENVIRONMENTS

An enhanced privacy-preserving outsourced classification algorithm for encrypted data is presented by Y. Chai et al. [13]. Their approach improves the security of outsourced categorization procedures, hence addressing important issues regarding data privacy. Through the use of encryption methods, the protocol guarantees the confidentiality of sensitive data while performing classification tasks, hence advancing safe data processing on wireless networks. A thorough secure data sharing system designed for cloud-edge computing scenarios is presented by Z. Song et al. [14]. Their research focuses on reducing the security threats related to data exchange across dispersed systems. The suggested technique provides improved protection for data sent between cloud and edge devices by putting strong security measures, such as encryption and access control mechanisms, into place. This strengthens overall system security.

A realistic and effective bidirectional access control method is put forth by J. Cui et al. [15] especially for cloud-edge data sharing scenarios. The difficulty of controlling access to shared data in dispersed systems is addressed by their work. The plan enhances access management in parallel distributed systems by enabling flexible and safe data exchange between cloud and edge devices through the introduction of a bidirectional control mechanism. Web Cloud, a web-based cloud storage system intended for safe cross-platform data sharing, is introduced by S. Sun et al. The goal of their research is to give consumers a simple, safe way to share data between many platforms and devices [16]. WebCloud enhances reliable safe computing in the cloud by enforcing the confidentiality and integrity of shared data through the use of authentication and encryption technologies.

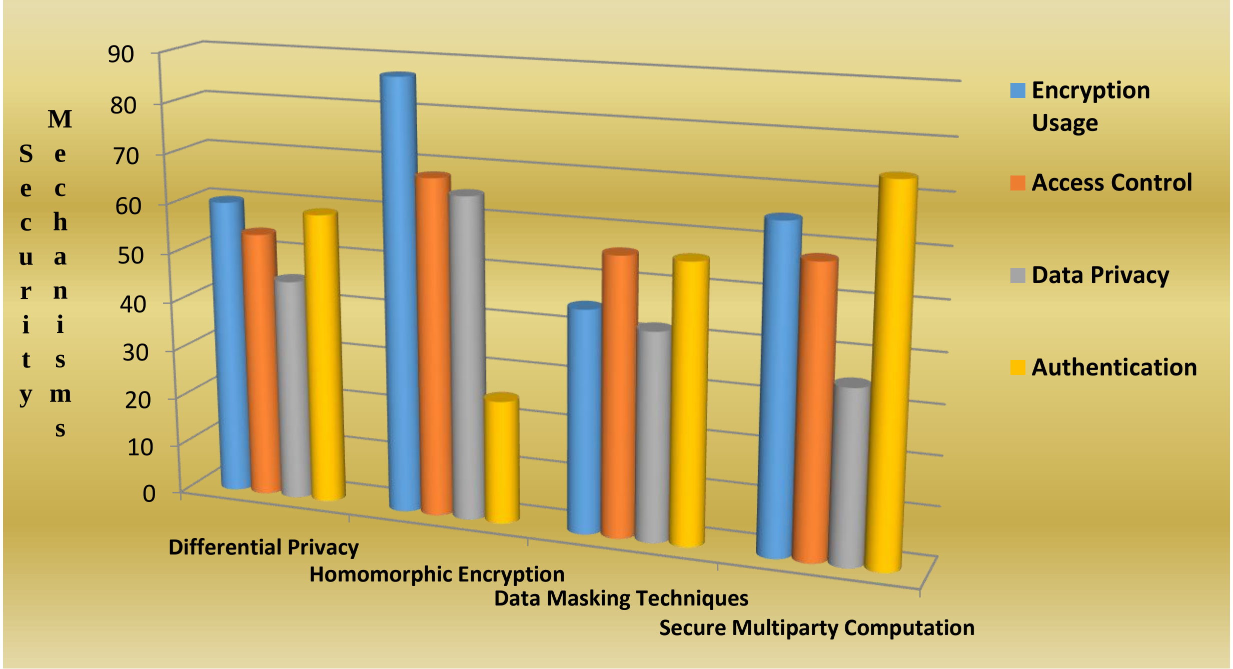
A trust-based secure multi-cloud cooperation framework for cloud-fog-assisted IoT settings is presented in the article by J. Zhang et al. [17]. Their research tackles the requirement for strong security protocols in cooperative IoT environments. The framework enhances security in cloud-assisted IoT ecosystems by enabling safe data sharing and cooperation among numerous cloud providers and fog nodes through the integration of trust-based procedures. For cloud-assisted Internet of Things settings, Q. Mei et al. provide expressive data sharing and self-controlled fine-grained data deletion procedures [18]. Their research is to improve control and privacy of data in Internet of Things devices. The suggested approaches enable users to manage their data more efficiently, improving security and privacy in trustworthy and secure computing environments by providing fine-grained control over data sharing and deletion.

Research on safe data sharing with adaptable user access permission updates in cloud-assisted IoMT is presented by J. Hao et al. [19]. Their research tackles the requirement for IoMT systems to have adaptive access control techniques. The suggested system allows for dynamic access control, which improves security in cloud-assisted IoMT contexts by permitting flexible privilege changes. A collaborative integrity auditing technique called CIA is proposed by T. Li et al. [20] for cloud data containing multiple replicas across many cloud storage providers. Their research is centered on making distributed cloud storage systems' data integrity safe. The suggested strategy improves data storage and retrieval operations in distributed and parallel systems by utilizing multi-replica storage and collaborative auditing techniques.

IV. RESULT AND PERFORMANCE ANALYSIS

The results of an extensive examination of the methods used to protect sensitive data, with a particular emphasis on four essential areas of cyber security data privacy, authentication, access control, and encryption usage are presented. It stands out as a popular option in terms of Differential Privacy, receiving exceptionally good ratings in every category. This method shows significant efficacy in protecting data privacy while upholding a sensible approach to authentication and access management. Homomorphic Encryption performs admirably, especially in the areas of encryption usage and access control. On the other hand, its effectiveness in authentication is comparatively lower, suggesting that there may be room for development in terms of safe user verification.

This method works well for basic data protection requirements, but for improved protection, it would need to be combined with more robust security methods. In the authentication space, Secure Multiparty Computation stands out as a strong competitor thanks to its greater capacity to safely validate user identities. Although it performs well in terms of encryption usage and access control, there is a noticeable space for improvement in terms of data privacy, indicating the need for further security measures to support secrecy. Overall, our research highlights the complexity of cyber security and the necessity for a thorough strategy that incorporates a range of methods to successfully reduce risks and protect sensitive data from ever-changing threats.



Graph.1 Graph for Comparative Analysis of Cyber security Techniques: Safeguarding Sensitive Data across Encryption, Access Control, Privacy, and Authentication

Security Mechanisms	Encryption Usage	Access Control	Data Privacy	Authentication
Differential Privacy	60	54	45	59
Homomorphic Encryption	87	68	65	25
Data Masking Techniques	45	56	42	56
Secure Multiparty Computation	65	58	35	74

Table.1 Classification table for comparative analysis of Cyber security Techniques

A wide range of aspects of developing technologies and approaches in network design, data privacy, security, and storage are covered in the ideas and research that are presented. Together, they help to solve important issues in their specialized fields. By streamlining the integration of IP and NDN networks, the suggested approach for movement from IP to NDN Using Double Channeled Translation Gateway improves scalability and efficiency for next network architectures. Comparably, investigating Big Data Privacy and Security Using Abundant Data Recovery Techniques and Data Obliviousness presents viable approaches to protecting private data in massive data settings while adhering to legal standards. Research on Threat Model and Defense Scheme for Side-Channel Attacks applies Client-Side De-duplication within the cloud storage security.

In cloud contexts, Lightweight Provable Data Possession with indistinguishable Obfuscation enhances data integrity and secrecy while reducing computational overheads for clients. It offers strong defenses against possible attacks. Furthermore, increasing effectiveness, accountability, and privacy preservation in cloud-based systems is made possible by the development of a Privacy-Preserving Public Auditing scheme for shared cloud data and the optimization of content caching strategies in hierarchical federated learning environments. The investigation of Multi-Keyword Ranked Searchable Encryption with support for Wildcard Keywords, which addresses important issues in cloud-based data repositories, improves data sharing capabilities while protecting user privacy and confidentiality. Together, these studies raise the bar in their domains, providing creative answers to urgent problems and opening the door for more effective, safe and privacy-conscious technology.

V. CONCLUSION

To sum up, the review of current research and recommendations in the fields of network architecture, data privacy, security, and storage shows notable progress and creative answers to urgent problems in these areas. The wide spectrum of research endeavors, ranging from enabling smooth transitions between network protocols to augmenting data privacy in expansive settings and strengthening security procedures in cloud storage systems, highlights the multifaceted character of modern technological breakthroughs. Together, these efforts aid in the development of systems that are more reliable, effective, and considerate of privacy. These studies open the door to the creation of more reliable and resilient infrastructures by tackling important issues including interoperability, regulatory compliance, security risks, and privacy protection. Future cooperation and research in these fields will be crucial for advancing technological advancement and guaranteeing

VI. REFERENCES

[1]. Du Ruizhong, Ma Caixia and Li Mingyue: Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains, Tsinghua Science and Technology, ISSNl1007-0214 02/18 pp13–26, DOI: 10.26599/TST.2021.9010070 Volume 28, Number 1, February 2023

[2]. Abdul Khaliq Awais and Anjum Adeel: A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy, Received March 2, 2022, accepted May 9, 2022, date of publication May 17, 2022, date of current version June 1, 2022. Digital Object Identifier 10.1109/ACCESS.2022.3175829.

[3]. Shakila Zaman and R. A. Khandaker Muhammad: Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare: Received January 28, 2022, accepted March 20, 2022, date of publication March 30, 2022, date of current version April 11, 2022. Digital Object Identifier 10.1109/ACCESS.2022.3163580

[4]. Fahrianto Feri: Migrating FromIP to NDN Using Dual-Channel Translation Gateway, received 8 June 2022, accepted 23 June 2022, date of publication 30 June 2022, date of current version 8 July 2022. Digital Object Identifier 10.1109/ACCESS.2022.3187421.

[5]. Funde Snehalata and Swain Gandharba: Big Data Privacy and Security Using Abundant Data Recovery Techniques and Data Obliviousness Methodologies, Received 30 July 2022, accepted 25 September 2022, date of publication 3 October 2022, date of current version 10 October 2022.Digital Object Identifier 10.1109/ACCESS.2022.3211304

[6]. Ha Guanxiong, Chen Hang, Jia Chunfu and Li Mingyue : Threat Model and Defense Scheme for Side-Channel Attacks in Client-Side Deduplication, TSINGHUA SCIENCE AND TECHNOLOGY ISSNl l 1 0 0 7 - 0 2 1 4 0 1 / 1 8 pp1 – 1 2 DOI: 10.26599/TST.2021.9010071 Volume 28, Number 1, February 2023

[7]. Chaudhari Smita and Swain Gandharba: Towards Lightweight Provable Data Possession for Cloud Storage Using Indistinguishability Obfuscation, Received February 17, 2022, accepted March 1, 2022, date of publication March 14, 2022, date of current version March 25, 2022. Digital Object Identifier 10.1109/ACCESS.2022.3159699

[8]. Khanal Subina, Thar Kyi and Huh Eui-Nam: Route-Based Proactive Content Caching Using Self-Attention in Hierarchical Federated Learning, Received February 7, 2022, accepted March 1, 2022, date of publication March 8, 2022, date of current version March 21, 2022. Digital Object Identifier 10.1109/ACCESS.2022.3157637

[9]. Kim Dongmin and Kim Kee Sung: Privacy-Preserving Public Auditing for Shared Cloud Data with Secure Group Management, Received March 30, 2022, accepted April 20, 2022, date of publication April 22, 2022, date of current version April 29, 2022.Digital Object Identifier 10.1109/ACCESS.2022.3169793

[10]. Jinlu Liu and others, Multi-Keyword Ranked Searchable Encryption with the Wildcard Keyword for Data Sharing in Cloud Computing, The Computer Journal, Volume 66, Issue 1, January 2023, Pages 184–196, https://doi.org/10.1093/comjnl/bxab153

[11]. T. Li, J. Zhang, Y. Shen and J. Ma, 2023 "Hierarchical and Multi-Group Data Sharing for Cloud-Assisted Industrial Internet of Things," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2023.3262563.

[12]. F. Rezaeibagha, Y. Mu, K. Huang, L. Chen and L. Zhang, "Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 217-228, 1 Jan.-March 2023, doi: 10.1109/TCC.2021.3087614.

[13]. Y. Chai, Y. Zhan, B. Wang, Y. Ping and Z. Zhang, "Improvement on a privacy-preserving outsourced classification protocol over encrypted data", Wireless Network., vol. 26, no. 6, pp. 4363-4374, 2020.

[14]. Z. Song, H. Ma, R. Zhang, W. Xu and J. Li, "Everything Under Control: Secure Data Sharing Mechanism for Cloud-Edge Computing," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2234-2249, 2023, doi: 10.1109/TIFS.2023.3266164.

[15]. J. Cui, B. Li, H. Zhong, G. Min, Y. Xu and L. Liu, "A practical and efficient bidirectional access control scheme for cloud-edge data sharing", IEEE Transaction Parallel Distributed Systems, vol. 33, no. 2, pp. 476-488, Feb. 2022.

[16]. S. Sun, H. Ma, Z. Song and R. Zhang, "WebCloud: Web-based cloud storage for secure data sharing across platforms", IEEE Transactions Dependable Secure Computing., vol. 19, no. 3, pp. 1871-1884, May 2022

[17]. J. Zhang, T. Li, Z. Ying and J. Ma, "Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1546-1561, 1 April-June 2023, doi: 10.1109/TCC.2022.3147226.

[18]. Q. Mei, M. Yang, J. Chen, L. Wang and H. Xiong, "Expressive Data Sharing and Self-Controlled Fine-Grained Data Deletion in Cloud-Assisted IoT," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2625-2640, 1 May-June 2023, doi: 10.1109/TDSC.2022.3188740.

[19]. J. Hao, W. Tang, C. Huang, J. Liu, H. Wang and M. Xian, "Secure data sharing with flexible user access privilege update in cloud-assisted IoMT", IEEE Trans. Emerg. Topics Computing, vol. 10, no. 2, pp. 933-947, 2022.

[20]. T. Li, J. Chu and L. Hu, "CIA: A Collaborative Integrity Auditing Scheme for Cloud Data with Multi-Replica on Multi-Cloud Storage Providers," in IEEE Transactions on Parallel and Distributed Systems, vol. 34, no. 1, pp. 154-162, 1 Jan. 2023, doi: 10.1109/TPDS.2022.3216614