A Review of Bidirectional Verification Techniques for Secure Storage in Cloud Computing

Dr. Ajay Jaiswal

Professor, Department of Computer Science and Engineering, K. D. K. College of Engineering, Nagpur
jaiswalajay1967@gmail.com; ajayjaiswal@yahoo.com

Abstract:

With cloud computing, you may significantly boost capacity or capabilities without investing in new equipment, hiring new staff, or purchasing new software. Cloud computing has developed over the past few years from a promising commercial concept to one of the fastest-growing segments of the IT industry. The cloud data centres are where the most delicate data and information are transported, where they are operated on virtual computing resources in the form of virtual machines. Security has emerged as a key concern in cloud computing, limiting its expansion while complicating data privacy and data protection issues continue to plague the industry. A new model developed for advancement shouldn't end up endangering the current model. When used in a cloud setting, the cloud architecture poses a serious danger to the security of current models. Users of various cloud services must be careful and aware of the possibility of data breaches in the new environment. This study presents an in-depth analysis of the different protected cloud storage options employing bidirectional protocols.

Keywords-- bidirectional protocols, security, virtual computing resources, virtual machine

DOI Number: 10.14704/nq.2022.20.13.NQ88248 **Neuro Quantology 2022; 20(13):1995-2000**

1. Introduction

The term "cloud computing" is used to describe this kind of computing as a business and personal IT architecture. Many organizations and people are signing up for cloud storage services like Dropbox and Google Drive. One of the key reasons why computers are so popular is because users can access their data from anywhere and share them with others with no effort. Security and privacy concerns are slowing the use of cloud storage. In spite of the fact that the leading cloud service providers utilize encrypted routes of communication and frequently decrypt data before employing it, the original data will still be available to the providers. That data is vulnerable to tampering and reading by anybody with access to the service provider's infrastructure. Individuals run the risk of having their privacy invaded, having their identities stolen, and having their safety compromised. The most efficient solution to this problem is to encrypt data on the client side before uploading it. The effectiveness of a cloud data system is largely determined by how well it stores and protects data. Concerning cloud-based safety: Any benefits of cloud computing are nullified if users are unable to trust the cloud's security measures to prevent their data from being stolen or their business from going under. Using the Cloud for Data Storage: Data warehouse expansion in the cloud should be approached with caution that it weaken existing cloud-based connections, given the volume of data available in the cloud While cloud data centers are more dependable and powerful than home computers, consumers' security worries still prohibit them from deploying their businesses to the cloud, slowing the industry's growth. The most obvious reason why customers are hesitant to trust cloud service providers with their data is the fear of relinquishing control of their information. Therefore, it is imperative that sensitive information stored in the cloud be shielded from prying eyes. Therefore, the data holder must confirm that cryptographic access control mechanisms will continue to guarantee the confidentiality of the outsourced data. Multiple data access control schemes have been offered by recent studies as a means of keeping cloud-based information safe. Data owners may safely manage authorized users and revoke authorization privileges with the use of such solutions .This study provides a comprehensive analysis of the state of bidirectional protocols for cloud-based safe storage.

Cloud computing is widely regarded as the IT industry's next major paradigm shift. Both hardware and software may be accessed from a central location in the cloud and then be made available to users whenever they need them through the web. To meet the demands of its users, a cloud environment makes use of remote data centres equipped with software and hardware to provide a variety of services across an appropriate network or internet [1] [2]. It's gaining popularity in many areas of technology due to its many advantages, including the elimination of the need to invest in infrastructure, the ability to scale down or up resources as needed, and the ability to pay only for the power actually consumed. There are many uses in mind for these benefits, which is why the cloud enterprise system has so many of them. Thanks to the cloud's convenient service, information may be accessed whenever and wherever it's needed. Since cloud computing relies on the interconnections of many individual computers, it inevitably features slow data processing and specialized connections. That's why the productivity and cost savings benefits of cloud computing make for an intriguing new paradigm of IT service deployment and maintenance.

2. Various security protocols of cloud computing

The cloud presents a wide variety of security risks and concerns. A number of the risks, difficulties, and challenges associated with cloud computing security are explored and their solutions proposed below. This leads to a challenge with authentication, as users of the cloud are likely to employ a variety of different login methods. Authentication at the user level is provided through the Single Sign-On. So that more information may be accessed quickly and easily, cloud infrastructure makes use of servers that are constantly adapting to user needs. To keep your cloud network secure, make sure to set up a virtual firewall and an intrusion prevention system (IPS). The cloud network's security is also managed from the central control panel. VPN, SSH, and SSL are all examples of virtual management clients. For the purpose of ensuring the security of cloud data, Sookhak et al. (2017) introduced a reliable remote data auditing method. In order to verify file integrity while minimizing computing burden on cloud clients and servers, this approach made use of algebraic features of the outsourced data blocks. For the purpose of facilitating real-time data updates with little overhead, a novel data structure was developed. The DCT data format allows the data owner to conduct operations such as modifying, erasing, appending, and joining on data at the block level rather than having to download the entire file. The suggested DCT structure is applicable for large-scale data sets and places little computing burden on auditors and servers. One streamlined technique was provided for remote data auditing that required minimal computational and network overhead. To ensure the safety of sensitive information stored in the cloud, Mohit et al. (2017) suggested a new standard mutual authentication protocol based on user authentication and a session key agreement technique. Through security analysis, the suggested method proved to offer superior protection over previously used methods. Performance metrics, like computation and computation overheads, were met with flying colors by the proposed protocol. An UML-based formal modeling and verification strategy for cloud computing protocols was provided by Fang et al. (2016). It included procedures for gathering requirements, creating a system architecture, and migrating data. To demonstrate the effectiveness and viability of the suggested solution, it was implemented in a real-world cloud-based conference management system. Using the foundation of UML 2.3 models, we improved the capacity to describe various perspectives and simplified formal modeling through automated transformation. An effective and fundamentally secure dynamic auditing technique was suggested by Yang et al. (2013). So, no extra containers or dividers were needed for this method. Multiple owners may be able to use the batch auditing protocol.

3. Secured cloud data storage

The front and back ends of a cloud service's architecture are two distinct parts. Using the network, the front and back ends may communicate with one another. The client or end user represents the front end, and the cloud service provider is at the back. Users can access cloud services via their own personal computers, which make up the front ends.

According to Boopathy et al. (2016), utilizing an E&DGS and a Digital Watermark Allocation and Verification Server, confidentiality of the data was ensured (DWA&VS). By using Automatic Data Backup Server, we were able to solve the problems with data accessibility and vendor lock-in (ADBS). If a user uploads a file that isn't compatible with the storage device, the Data Type Identification (DIT) system will flag it and prevent the upload. But hackers may target any server, potentially removing all of the data and information stored there. Data encryption prevents users from reading it in their native format. For the reversal to be completed, the data must eventually arrive at either the E&DGS or the DWA&VS. In 2016, Vurukonda et al. introduced a distributed cloud data storage framework that offered a safe access advantage over cloud information such as FADE. The concepts of time-based guaranteed deletion and Vanish data are explained. This ensures that the documents made possible by modern distributed storage systems may be deleted without a trace, provided that the appropriate permissions are granted to do so. A third-party auditor is available for consumers under the public auditability paradigm, as outlined by Hsien et al. (2016). The public auditability needs that were most essential for this application's use case were sorted out. In 2017, Shin et al. developed an efficient solution for reducing data storage needs in the cloud without compromising data privacy or security. This study investigated and contrasted several implementations of the scheme, analysing their strengths and weaknesses in terms of efficiency and security. Deduplication systems and their benefits are generally acknowledged by most current cloud service providers; however numerous practical problems exist about the security and privacy of cloud data. Identity-based distant data integrity checking was a novel primitive studied by Yu et al. (2017) for safe cloud 11 data storage. This primitive's soundness and complete data privacy, two crucial qualities, have been codified in a security model. The suggested protocol was shown to be efficient and workable by numerical analysis and actual implementation.

4. Data Security during transmission

Gai et al. (2017) developed a unique cloud-based approach for transferring multimedia data from automobiles in real time during VCS implementation. Data packets might potentially be dynamically allocated to cloud resources based on stringent security requirements, as investigated by the suggested technique. The suggested solution not only protected private information, but also increased the total security level, which previously relied on the effectiveness of cloud servers. Experiment results confirmed the adaptability and viability of the proposed strategy. Zhao et al. designed and implemented a secure framework for spreading MapReduce tasks over several nodes (2014). It's feasible that users will utilise the single sign-on feature made available by the security framework to send tasks to G-Hadoop. The safety procedures relied on either proven methods of security, such SSL and cryptographic algorithms, or on the theory behind those methods, like GSI. Data safety was prioritized in the design of a data placement approach proposed by Liu et al. (2014), which would automatically disperse data sets among data centres. This strategy was put into action by looking at the security model for scientific workflow systems from the service provider's, the end user's, and the evaluation's points of view. A security model was developed to enable the quantification of data centre security services. An ACO-based algorithm was utilised to dynamically determine which data centres were most suited to guarantee the continuous security of data. The goal of this research was to investigate methods to reduce the data sent between data centres, but it gave little regard to issues like security, cost, and other constraints. Cloud computing allows customers to store their information and programmes remotely and pay only for the time they actually use them. Fang et al. (2015) examined the problem of cloud computing's high total energy usage by examining factors including the energy required for data transport. The transmission scheduling issue in cloud computing is a stochastic optimization problem with the goal of minimizing the combined utility of network energy cost and the dropping penalty while meeting the different application requirements.

5. Data integrity and Data Confidentiality

Cloud customers must prioritise both data privacy and data integrity. Encryption is helpful in protecting sensitive data, but it cannot detect whether data has been altered during cloud storage. The two main tools for protecting information are the Message Authentication Code (MAC) and the Digital Signature (DS). MAC uses a symmetric key to compute a check sum that is attached to the information for security purposes. The DS method, on the other hand, relies on the public key infrastructure to function (Having public and private pair of keys). Since symmetric algorithms are much quicker than asymmetric algorithms, we consider Message Authentication Code (MAC) is the best alternative to offer the integrity checking method. Data integrity assurance is particularly important in this context since there is evidence that PaaS and SaaS don't provide any integrity protection.

6. Bidirectional Verification Protocol

Since cloud storage covers a broad range of data, it has the potential to be utilised in many different contexts, provided that proper safety precautions are taken. In this study, we analysed how different cloud services handle security for their stored data. The benefits of the various protocols used for encrypted data transfer in the cloud are discussed. Data transmission protocols, such as those for bidirectional verification, auditing, etc., are discussed in detail for the cloud.

7. Methods

Here, we present an encrypted keyword search (APKS) for use in the cloud. We introduce an offline, encrypted search system where users get their query strength from local authorities who have good user ratings thanks to their trustworthy attributes. Next, we suggest two innovative APKS solutions, one of which is highly efficient and the other of which is encrypted, both of which are based on the most recent cryptographic primitive encryption, hierarchical predicate (HPE) encryption. In addition to protecting both the content and the queries, our programmes also provide multi-sided keyword support that functions with a number of basic queries, enabling the submission and acquisition of search capabilities. We implement our technology in a contemporary office setting, and the results of our tests demonstrate its viability in the real world. [4]

Safeguarding Individual Privacy in Electronic Health Records through Access Control Elimination and Encryption. We propose that cryptography and permission management be used to ensure the safety of such systems. To further ensure patient privacy in the event of a compromised host data centre, we also reject systems that permit patients to produce and store encryption keys. One typical criticism of this approach is that encryption would reduce system efficiency. It does, however, demonstrate that it is possible to develop a reliable system that enables patients to grant others limited access to their records and to do searches within those records. We have completed the Patient-Managed Encryption System's formal implementation criteria and delivered a few presentations based on the available concealed resources and agreements, with each presentation receiving its own unique set of features.

Over the course of several decades, cloud computing has evolved as a research tool for fields such as virtualization, distributed computing, utility computing, networking, web development, and software services. The term "cloud computing" refers to a service-oriented architecture that is intended to lessen the burden of IT on the end-user by, among other things, reducing costs and making IT more adaptable to changing needs. The author [21] discusses the approach taken by cloud computing to address the challenges, as well as associated research areas and the necessity of cloud. Grid computing, parallel computing, virtualization technology, utility computing, and other computer technologies have all contributed to the development of cloud computing. Large-scale processing, data storage, virtualization, high dependability, and low cost are some of cloud computing most distinguishing features. Cloud computing rapid expansion may be stymied by concerns over data security. This paper's [22] primary objective is to introduce cloud computing systems and, using cloud computing's concepts and personalities, assess cloud computing's security challenges. Data privacy and service availability are at the heart of the security issue with cloud computing. The cloud computing system needs to be protected using a wide variety of security measures, both old and modern. Through the usage of cloud computing, capabilities can be increased without the need to purchase additional hardware, get software licences, or train additional staff. Due to cloud computing, IT is now able to last for much longer. It's a winning strategy for doing business, thus it's growing quickly in the IT sectors. Businesses and consumers alike are increasingly worried about how safe their data is when it's kept in the cloud. There is a growing interest in cloud computing, but most businesses are hesitant to move their data there just yet [23]. Cloud computing's expansion was slowed by security concerns, which in turn are dominated by concerns over data privacy and protection. Existing models in cloud computing do not include all of the features needed for the launch of the advanced model. This new model is meant to fix the problems with the old one, but it shouldn't water down any of the essential parts. When used in a cloud setting, cloud architecture poses a threat to the safety of current technology. Users of cloud services need to be aware of the potential dangers in this new setting. The author of [24] suggests a review of the many cloud security vulnerabilities that have been presented. Cloud computing service delivery and related security concerns are represented. The data is encrypted using industry-standard algorithms before it is sent to the cloud computing service, while it is being stored there, and while it is being transmitted. A wide variety of algorithms, including Identity-Based Encryption [35, 36], Key Policy Attribute-Based Encryption [37, 38], Cipher text-Policy Attribute-Based Encryption [40], and Hierarchical Attribute-Based Encryption [39, 40], are utilized. Both full delegation and fine-grained access control over attributes are supported by these cypher systems.

CONCLUSION

The use of cloud computing to store and transfer data is a promising and expanding industry. The rapid expansion of cloud computing is being met with increasing resistance, with security and privacy emerging as the two most pressing concerns. Since data and information exploration is so important for making decisions, it is crucial for any firm to minimise data storage and cut processing costs. Thus, techniques have been presented for the same problem, such as data security and protection in the cloud, and the business organization expects a high level of confidence between the business owners and the cloud service providers before transferring any data to the cloud. However, in order for cloud service consumers to embrace cloud computing, the methodologies and approaches used to do so must be made more efficient and powerful. In this research, we examine the trustworthiness between customers and cloud service providers by exploring several approaches and methodologies focused on data privacy and security on cloud storage**.**

References

[1] Sravanthi, M., &Bhaskar, N. (2016). Shared Authority Based PrivacyPreserving Authentication Protocol in Cloud Computing.

[2] Tamrakar, S., Hoang, L. N., Pendyala, P. K., Paverd, A., Asokan, N., & Sadeghi, A. R. (2015). OmniShare: Securely accessing encrypted cloud storage from multiple authorized devices. CoRR, abs/1511.02119.

[3] Gupta, S., & Xaxa, M. D. K. (2016). Cloud Security based on ECCDiffie-hellman Protocol and Storage Optimization using compression.

[4] Sookhak, M., Yu, F. R., Khan, M. K., Xiang, Y., & Buyya, R. (2017). Attribute-based data access control in mobile cloud computing:

Taxonomy and open issues. Future Generation Computer Systems, 72, 273-287.

[5] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[6] Ren, Y. J., Shen, J., Wang, J., Han, J., & Lee, S. Y. (2015). Mutual verifiable provable data auditing in public cloud storage. 16(2), 317-323.

[7] Joshi, B., Joshi, B., & Rani, K. (2017). Mitigating Data Segregation and Privacy Issues in Cloud Computing. In Proceedings of International Conference on Communication and Networks (pp. 175-182). Springer, Singapore.

[8] Sookhak, M., Gani, A., Khan, M. K., & Buyya, R. (2017). Dynamic remote data auditing for securing big data storage in cloud computing. Information Sciences, 380, 101-116.

[9] Mohit, P., Amin, R., Karati, A., Biswas, G. P., & Khan, M. K. (2017). A standard mutual authentication protocol for cloud computing based health care system. Journal of medical systems, 41(4), 50.

[10] Fang, K., Li, X., Hao, J., & Feng, Z. (2016, August). Formal Modeling and Verification of Security Protocols on Cloud Computing Systems Based on UML 2.3. In Trustcom/BigDataSE/I SPA, 2016 IEEE (pp. 852-859). IEEE.

[11] Yang, K., & Jia, X. (2013). An efficient and secure dynamic auditing protocol for data storage in cloud computing. IEEE transactions on parallel and distributed systems, 24(9), 1717-1726.

[12] Boopathy, D., & Sundaresan, M. (2016). Secured Cloud Data Storage––Prototype Trust Model for Public Cloud Storage. In Proceedings of International Conference on ICT for Sustainable Development (pp. 329-337). Springer Singapore.

[13] Vurukonda, N., Rao, B. T., & Reddy, B. T. (2016). A secured cloud data storage with access privileges. International Journal of Electrical and Computer Engineering, 6(5), 2338.

[14] Hsien, W. F., Yang, C. C., & Hwang, M. S. (2016). A Survey of Public Auditing for Secure Data Storage in Cloud Computing. IJ Network Security, 18(1), 133-142.

[15] Shin, Y., Koo, D., & Hur, J. (2017). A Survey of Secure Data Deduplication Schemes for Cloud Storage Systems. ACM Computing Surveys (CSUR), 49(4), 74.

[16] Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2017). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), 767-778.

[17] Yadav, D. S., & Doke, K. (2016). Mobile Cloud Computing Issues and Solution Framework.

[18] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing, 63(2), 561-592.

[19] Meenakshi, K., & George, V. S. (2014). Cloud server storage security using TPA. International Journal of Advanced Research in Computer Science and Technology.

[20] Garg, N., & Kaur, K. (2016). Hybrid information security model for cloud storage systems using hybrid data security scheme. International Research Journal of Engineering and Technology (IRJET), 3(04).

[21] Kuila, S., Shridhar, S., Patel, C., & Iyengar, N. C. S. (2016). Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management. Journal of Computer and Mathematical Sciences, 7(11), 558-565.

[22] Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.

[23] Gai, K., Qiu, L., Chen, M., Zhao, H., & Qiu, M. (2017). SA-EAST: security-aware efficient data transmission for ITS in mobile heterogeneous cloud computing. ACM Transactions on Embedded Computing Systems (TECS), 16(2), 60.