International Journal of Engineering & Technology, 7 (4.36) (2018) 511-514

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Review on Secure Storage Using Bidirectional Verification Techniques in Cloud Computing

Mr. Girish kumar d[1], dr. Rajashree v biradar[2], dr. V c patil[3]

[1]*Research Scholar, Department of CSE, BITM, Ballari, Karnataka, India*
[2]*Professor Department of CSE, BITM, Ballari, Karnataka, India*
[3]*Principal, BITM, Ballari, Karnataka, India*

Abstract

Cloud computing increases the capacity or capabilities vigorously without devoting new infrastructure, training new personnel, or licensing the new software . In the past few years, cloud computing has grown from being a promising business concept to one of the fast-growing sectors of IT industry. As the more sensitive information and data are moved into the cloud data centers, they run on virtual computing resources in the form of virtual machines. Security has become one of the major issue in cloud computing which reduces the growth of cloud environment with complications in data privacy and data protection continue to outbreak the market. A new model created for the advancement should not result as a threat to the existing model. The architecture of cloud poses such a threat to the security of existing models when deployed in a cloud environment. The different cloud service users need to be attentive in considerate,about the risk of data breaks in the new environment. In this paper, advanced survey of the various secured storage in cloud computing using bidirectional protocols is presented.

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

1. Introduction

Cloud computing is referred to as Information Technology (IT) architecture for both the enterprise and individuals. The cloud storage services such as Dropbox, and Google Drive, are increasingly being used by the individuals and various kind of businesses. The main reason behind the wide preference of computing is given as, i) the possibility to use files from several devices or locations, ii) the ability to easily share the document with others. The data privacy and security is restraining the acceptance of cloud storage services.Even though the major cloud service providers use secure communication channels and routinely encrypt the data before using it, the original data will be still accessible to the service providers. Anyone with access to the service provider's infrastructure, could read and modify the data. This leads to loss of privacy, identity theft, and security for individuals. Encrypting the data from client side before uploading is the effective way to overcome this issue (Tamrakar et al. 2015). The storage and the security in cloud computing are the two main aspects which decides the efficiency of the cloud data system.

Security in cloud: Failing to authorize the security protection, once the mistreatment cloud service might eventually end in higher worth and potential loss of the business, hence eliminate any of the potential edges of cloud computing.

Storage in Cloud Environment: Huge data that exists on the cloud, therefore ought to astuteness to make sure that data warehousing is increased and does not transform a frail affiliation in cloud stage (Gupta et al. 2016). Cloud data centers are more reliable and powerful while compared to the personal computers, still the security concerns prevent the users to deploy their business in the cloud and thus reduces the growth of cloud computing. The most apparent reason is that the users are not willing to delegate the management of data to a cloud service provider is that they lose their physical control over the outsourced data. So, the sensitive data in cloud storage must be protected from the unauthorized access. As a consequence, the data holder needs to certify that the concealment of the outsourced data remains protected by using cryptographic access controlsystems. Recent researches have proposed several data access control scheme to protect the stored data in cloud computing. Such systems permit the data owner to securely handle authorized users and retract the permission rights (Sookhak et al. 2017). This research presents a review of secure storage in cloud computing by using bidirectional protocols.

2. Literature Review

2.1. Cloud computing applications

Almorsy et al. (2016) described that cloud computing model was one of the promising computing models for the service providers, cloud providers, and cloud consumers. The cloud security problems are given as follows: i) Some security problems were inherited from the used technologies such as virtualization and SOA, ii) Multi-tenancy and isolation was a major dimension in the cloud security problem that required a vertical solution from the SaaS layer down to physical infrastructure, iii) Security management was critical to control and manage the number of requirements and controls. Ren et al. (2015) proposed the mutual verifiable data possession scheme. The MV-PDP system model andsecurity model was defined and DiffieHellman shared key was utilized to construct the homomorphic authenticator. In MV-PDP, the data blocks signed by a client could be verified by a private verifier, while the data bocks signed by a verifier could also be checked by the client. Song et al. (2017) defined and solved the problem of supporting efficient privacy preserved full text

retrieval to enrich the query function over the encrypted cloud data. A word based hierarchical bloom filter tree index structure was designed to execute the full text retrieval over the encrypted documents at the cloud. A ranking algorithm was designed to effectively utilize the valuable bandwidth resource. By means of the security and performance analysis, the proposed research solution was secure and privacy preserving, while realizing the goal of the full text retrieval over the cloud encrypted data. Joshi et al. (2017)suggested that cloud computing helps to reduce the cost, management responsibilities, maintenance, and increase the efficiency of the resources. This research mainly focused on Data Storage issues, which provided security and confidential data to the users.

2.2. Various security protocols of cloud computing

Sookhak et al. (2017) presented an effective remote data auditing scheme to verify the integrity of the data stored in cloud computing. This method employed algebraic properties of the outsourced data blocks to check the integrity of files, and reduce the computational overhead on the client and server side of the cloud. A new data structure was deigned to support dynamic data update which acquires reduced computational and communication costs. With the aid of DCT data structure, the data owner could perform modify, delete, insert, or affix the procedures at block level without downloading the whole file. The proposed DCT structure could be applied for huge scale data and will incur least computational cost on the auditor and server. A single remote data auditing method was presented which incurred minimum processing time and communication overhead. Mohit et al. (2017) proposed a new user authenticated and session key agreement scheme, standard mutual authentication protocol for cloud data security. The proposed technique provided better security than other existing schemes through security analysis. The proposed protocol was efficient in terms of performance, such as computation and computation overheads. Fang et al. (2016) presented an UMLbased formal modeling and verification approach which covered the requirements capture, system design and converting steps of cloud computing protocols. This approach was applied to the practical cloud based conference management system to prove the efficiency and feasibility of the proposed method. On the basis of UML 2.3 models, the description ability of different view was enhanced and the complexity of formal modeling by automatic transformation was reduced. Yang et al. (2013) proposed an efficient and inherently secure dynamic auditing protocol. Thus, this technique did not require any additional organizer. The batch auditing protocol could also support batch auditing for multiple owners.

2.3. Secured cloud data storage

Boopathy et al. (2016) described that data confidentiality was assured using Encryption and Decryption Gateway Server (E&DGS) and Digital Watermark Allocation and Verification Server (DWA&VS). The data availability and vendor locked in issues were eliminated by deploying Automatic Data Backup Server (ADBS). The Data Type Identification (DIT) avoids the mismatched file format uploads, and the data becoming vulnerable due to the storage user. But any of the server may be attacked by the hackers and they might take out the information and data from that particular server. The encrypted data requires decryption to know exactly what it contains. The data must reach the E&DGS or DWA&VS to complete the reversing process. Vurukonda et al. (2016) presented a distributed cloud data storage background that guaranteed secure access benefit over cloud information like FADE.It describes about the Time-based file assured deletion and Vanish data.This provides access control guaranteed erasure to the documents that were facilitated by today's distributed storage administrations. Hsien et al. (2016) described that in public auditability model, the users could go for the third party auditor to verify the data efficiency. The basic requirements of the public auditability which could be classified to the case of the particular application was sorted out. Shin et al. (2017) described an effective method for minimizing the cloud storage space while preserving the security and privacy of the cloud data. This research analyzed and compared in terms of efficiency and security, and provided the advantage and disadvantage of the scheme. Even though the deduplication systems and their benefits are broadly accepted by most of the present cloud service providers, there exist many practical concerns regarding the security and privacy of the cloud data. Yu et al. (2017) investigated a new primitive known as identity based remote data integrity checking for secure cloud 11 storage. The security model of the two important properties of this primitive such as soundness and perfect data privacy was formalized. The numerical analysis and the implementation showed that the proposed protocol was efficient and practical.

2.4. Privacy & Security in cloud computing

Yadav et al. (2016) described cloud computing as a restoration of the classic mainframe client server model. The resources were pervasive, ascendable, and highly virtualized. Modi et al. (2013) attempted to display various vulnerabilities, threats, and attacks deterring the adoption of cloud computing. The existing algorithms were tested to address the security issues at various layer of cloud, while identifying some problems. This research included a need for dynamic security model and better crypto algorithms targeted at different levels of security and privacy for cloud computing. The TPA could be used to ensure the security and integrity of the data. TPA acts as a trusted third party to resolve the conflict between the cloud service provider and the client. Garg et al. (2016) adopted the hybrid approach for securing the data storage on cloud. Due to the increase in development of internet technology, it is necessary to secure the data stored by the user on the cloud and maintain their confidentiality. The loaded image has been encrypted and the cover image was used to hide it, so the observers were unable to get the original content. Kuila et al. (2016) proposed an OTP and blowfish algorithm based security for the cloud data. By generating the OTP, increases more reliable verification system. Chang et al. (2016) demonstrated the integrated security approach and its advantages of cloud computing. The motivation and the related survey about the CCAF security was explained and the core technologies were described that considered enterprise security concerns and addressed EFSS security issues. The CCAF security was presented with the integration of three layered security such as firewall, identity management, and encryption. Several experiments were designed for demonstrating CCAF multi-layered security as a working framework for the business clouds. The results showed that CCAF multi-layered could detect and block 9995 virus attacks, and trojans during the penetration test and could block above 85% of attacks for 100 hours. The CCAF security policy could work with real time examples and also could align with the businesses to protect the data.

2.5. Data Security during transmission

Gai et al. (2017) proposed a novel cloud based approach which supported real time vehicular multimedia data transmissions while implementing VCS> The proposed model was an exploration of dynamically assigning data packet to cloud resources based on the security requirements. By implementing the proposed technique not only protected the sensitive data but also increased the entire security level which depended on the cloud server performance. The experimental evaluation proved the feasibility and adaptability of the proposed technique. Zhao et al. (2014) designed and implemented a security framework for running MapReduce tasks across different clusters in a distributed environment. The security framework provided users with single

sign on process to submit jobs to G-Hadoop. The security mechanisms were based on some present security solutions such as SSL and cryptographic algorithms, or the concept of other security solutions such as GSI. Liu et al. (2014) proposed a data placement strategy that could automatically allocate datasets to datacenters in order to improve the data security. This strategy was executed by analyzing the security model for scientific workflow systems from the service providers, service consumers, and service evaluation.A security model was introduced to quantitatively measure the security services which are provided by the data centers. To dynamically select the appropriate data centers for immediate data security, ACO based algorithm was utilized. This research focused on reducing the data transmission across the data centers and rarely considered the security constraints, cost, and other factors. Cloud computing provided a pay demand computing model where the user could access the applications and data from anywhere of the world. Fang et al. (2015) investigated the energy consumption problem in cloud computing such as energy for data transmission. The transmission scheduling problem in cloud computing was formulated as a stochastic optimization problem, whose objective was to minimize the joint utility of network energy cost and the dropping penalty while satisfying the different application requirements.

2.6. Bidirectional Verification Protocol

Feng et al. (2016) proposed a remote data auditing system that supported bi-directional verification and further validated for the data security in cloud . A new entity was utilized to generate the authority's credentials, so that no longer has to assume that each TPA was credible. The CSP could verify the authority of verification party and rejected the requests that come from unauthorized users. The allocation of the computational overhead was optimized and greatly reduced the computational overhead of the client. The CSP would actively transfer the computing overhead to the verification party if CSP's computing power was not sufficient to provide service to all users. An additional validation scheme was presented to solve the problem of file errors. Husain et al. (2014) presented a multipurpose storage enforcing remote verification scheme that utilized polynomial hash for cloud storage verification. Sookhak et al. (2017) discussed the access control systems and a wide range of attribute based access control mechanisms applied in cloud computing

3. Comparative Table

Sl. No	Author Name, Year	Title of the paper	Protocol used	Advantages	Research Gap
1	Ni et al. (2014)	On the security of an Efficient Dynamic Auditing Protocol in Cloud Storage	Dynamic and privacy preserving auditing protocol	This study demonstrated that an active adversary can modify the auditing proof	Remedy was suggested without losing any features of the original protocol
2	Gai et al. (2017)	SA-EAST: Security-Aware Efficient Data Transmission for ITS in Mobile Heterogeneous Cloud Computing	Cloud-based approach supporting real-time vehicular multimedia data transmission was proposed	This research explored dynamically assigning data packet to cloud resources based on security requirements	Two main algorithms in SA-EAST were CRM and SCRA Algorithms for future research direction
3	Cao et al. (2014)	Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel	Single Sign on Protocol was proposed	A proxy was designed to allow and support a smooth transition from existing SSO protocol to the proposed protocol	Strong security guarantees are lagging which could be the future research gap
4	Gupta et al. (2016)	Cloud Security based on ECC-Diffie-hellman Protocol and Storage Optimization using compression	Diffie hellman protocol was proposed	The error rate obtained was minimum than the existing method. The Average Error rate was 2.94% and the Average value of Entropy value that was defining the Security of encrypted data was 93.81%	Several combination of key size factors leads to further improvement
5	Chen et al. (2016)	Secure Cloud Storage Meets with Secure Network Coding	Generic secure cloud storage protocol based on secure network coding protocol	Publicly verifiable secure cloud storage protocol which was secure without the use of random oracle heuristic was obtained	New secure cloud storage protocols based on generic construction and existing/ future researches on secure network coding protocols can be directed as research gap
6	Jain et al. (2017)	Cloud Security Protocol Identifying Users without Login Id	QR code protocol	Secured method and only authorized person can encrypt and retrieve the secret code from QR code	During authentication the login id is not asked and so the stolen password cannot be used. Security measures could be deployed to the authentication process

4. Conclusion

Cloud, being the wide band of data storage system could be used in various applications by deploying appropriate security measures. This research study discussed the various secured data storage systems in cloud computing. Different protocols adopted for the secured data transmission in cloud is addressed with its advantages. The various protocols for effective cloud data transfer such as bi-directional verification protocol, auditing protocols, etc. are described.

References

[1] Sravanthi, M., &Bhaskar, N. (2016). Shared Authority Based Privacy-Preserving 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 ECC-Diffie-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.

[24] Zhao, J., Wang, L., Tao, J., Chen, J., Sun, W., Ranjan, R., ... & Georgakopoulos, D. (2014). A security framework in G-Hadoop for big data computing across distributed Cloud data centres. *Journal of Computer and System Sciences*, *80*(5), 994-1007.

[25] Liu, W., Peng, S., Du, W., Wang, W., & Zeng, G. S. (2014). Security-aware intermediate data placement strategy in scientific cloud workflows. *Knowledge and information systems*, *41*(2), 423-447.

[26] Fang, W., Yin, X., An, Y., Xiong, N., Guo, Q., & Li, J. (2015). Optimal scheduling for data transmission between mobile devices and cloud. *Information Sciences*, *301*, 169-180.

[27] Feng, B., Ma, X., Guo, C., Shi, H., Fu, Z., & Qiu, T. (2016). An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing. *IEEE Access*, *4*, 7899-7911.

[28] Husain, M. I., Ko, S. Y., Uurtamo, S., Rudra, A., & Sridhar, R. (2014). Bidirectional data verification for cloud storage. *Journal of Network and Computer Applications*, *45*, 96-107.

[29] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences*, *258*, 371-386.

[30] Ni, J., Yu, Y., Mu, Y., & Xia, Q. (2014). On the security of an efficient dynamic auditing protocol in cloud storage. *IEEE Transactions on Parallel and Distributed Systems*, *25*(10), 2760-2761.

[31] 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.

[32] Durga, B.K., Rajesh, V. "Review of facial emotion recognition system",(2018) International Journal of Pharmaceutical Research, 10 (3), pp. 94-100.

[33] Cao, Y., Shoshitaishvili, Y., Borgolte, K., Kruegel, C., Vigna, G., & Chen, Y. (2014, September). Protecting web-based single sign-on protocols against relying party impersonation attacks through a dedicated bi-directional authenticated secure channel. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 276-298). Springer, Cham.