WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey of Data Sharing and Privacy Preserving Policy of Cloud Computing with Security

Prof. Kamble D. R *

Department of Computer Engineering, SBPCOE, Indapur, 413106 India

ABSTRACT

People approve the incredible power of cloud computing but cannot fully trust on cloud providers due to the absence of user-to-cloud controllability. The Attribute Encryption Standard (AES) is used to share and secure the encrypted file with different users. On cloud the user stores their sensitive data without direct control, so there is less security over the data. There are many chances for the hacker to consume the resources, modify the data or to corrupt the data. So, the proposed system overcomes all these issues; to keep data secure from hacker. We use a privacy-preserving access policy for secure communication and maintaining confidentiality for secure data access and transfer. SHA 512 is used for generating the hash function and authentication in the system. Therefore, providing security for the data sent over the internet is necessary. The owner and user of the server raise many issues without direct control. In this work, we take one middleware, the authority that verifies the user's request and gives the encryption key directly to the user via mail to obtain resources from the cloud. No one can modify data without user permission. This empowers every user and each authority specialist to claim and control their data associated with the user's documents inside a protected situation. The proposed system state that, for secret communication with the cloud. The data is given to the owner, and the hash is given to the authority. The user gets the encryption key to access the cipher text.

Keywords: Cloud Computing; error localization; erasure code; AES; Steganography; encryption.

1. Introduction

Cloud computing is used through the internet, which enables the distribution of services. Today, cloud computing is the most important concept that people advocate for the incredible power of cloud computing, but the lack of control from the user to the cloud makes it impossible to fully trust the cloud provider. To share encrypted files with others, you can use Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enforce fine-grained, owner-centric access control. However, this is not secure enough against other attacks.[1] Malicious attackers can download thousands of files and launch EDoS (Economic Denial of Sustainability) attacks that consume a lot of cloud resources. Cloud computing concepts also include general terms such as data-as-a-service and everything-as-a-service. [2] Attribute-based encryption (ABE) [3] is considered one of the most appropriate techniques for enforcing and managing data usage rights in public clouds, as it allows data owners to commit to direct control over their data. increase. Many kinds of his ABE algorithms are currently proposed, divided into two categories: key policy attribute-based encryption (KP-ABE) [3] and ciphertext policy attribute-based encryption (CP-ABE). The benefits of cloud computing are immense, but security and privacy concerns remain major barriers to widespread adoption. While CSP infrastructure and management capabilities are far more powerful and reliable than personal computing devices, cloud platforms are still prone to media failures, software bugs, malware, administrator error, and malicious insider attacks. [5] The cloud brings many advances in hardware and software applications for data management, seen in precise accessibility. However, cloud computing has many issues in terms of data security, which is one of the biggest problems in adopting data in cloud environment. Therefore, the work proposed here relinquishes data and security controls and employs several mitigation techniques against attacks. Focus on cloud data security, storage, protect system and data. We propose a strict distributed scheme against attacks.

2. Related Work

[1] Xue, K., Chen, W., Li, W., Hong, J., & Hong, P- People recognize the incredible power of cloud computing, but the lack of user-to-cloud control prevents them from completely trusting cloud providers. To ensure confidentiality, data owners should upload data, not in plain text. To share encrypted files with others, you can use attribute-based ciphertext policy (CP-ABE) encryption algorithms to enforce fine-grained, owner-centric access control. However, this is not very secure against attackers. Here, a malicious attacker attacks the cloud, downloads thousands of files from the cloud, and launches her EDOS (denial of economic sustainability) attack that heavily consumes the cloud resources. Cloud server providers are the main players in providing services, accountants and payees for resource consumption fees and ensuring billing to owners. This work applied security to cloud storage using the CP-ABE algorithm to mitigate EDOS attacks. [1].

[2] Sivasakthi, T., & Prabakaran, D. N**.-** Cloud computing is used over the Internet to share software information and resources with the world. Share resources for all servers and all users independently. This digital signature uses user authentication of secure data using the cloud computing digital signature encryption algorithm. This allows you to keep your information in the cloud, handle all your sensitive data, and keep all your documents safe with digital signatures, as all important documents that are signed are not physically secure. You can do this by using a cryptographic algorithm that shares a key with both the sender and receiver. We have applied security to your data based on the internet using encryption algorithms RSA, AES, SHA. To protect against attackers, use encryption and encryption algorithms [2].

[3] Li, W., Xue, K., Xue, Y., & Hong, J.- In this paper, a Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storages. In this work, Attribute-Based Encryption (ABE) was used as the best algorithm and performed directly by the data owner. We guarantee the tools to You are promised control over your data in public cloud storage. TMACS (Training and Management Access Control) is a system that is not only proven to be secure, but also robust when permissions are active within the system. It uses the ABE and CP-ABE encryption algorithms to maintain the entire attribute set, creating a single bottleneck in both security and performance. After that, several systems with some powers have been proposed. In this system, permissions manage separate sets of disjoint attributes. TMACS is a system that satisfies attribute schemas from various agencies and provides robustness at the security and system level [3].

[4] Somani, Gaurav, Manoj Singh Gaur, and Dheeraj Sanghi.- In this work, DDoS attacks have recently become malicious attacks. This is a direct attack on the cloud, consuming all resources and causing economic loss. Her next DDOS attack is the EDos (denial of economic sustainability) attack. Direct impacts of distributed clients/bots. This is typically achieved by targeting one or more basic server resources such as CPU, memory, disk, and bandwidth.For example, the number of TCP connections. It was used to understand the impact of DDoS/EDoS attacks in the cloud [4].these attacks on other stakeholders include service disruption, web service performance, resource contention, indirect EDoS, downtime, and business loss. A distributed denial of service (DDoS) attack is a targeted attack against a victim server being attacked cooperatively or uncooperatively by a large number of service requests from a group of

[5] Ren, K., Wang, C., & Wang, Q.- Cloud computing is the latest term for the long-awaited vision of computing as a utility. The cloud offers flexible on-demand access control, policy and security. Cloud computing has many security issues. Identifying the attacker is very difficult. The attacker's location could be an insider, an outsider, or a malicious attacker. It attacks the cloud, subverts all security and consumes resources without permission. CSP also grants access without knowledge of existing users. While this is a critical security challenge, here the authors outline some critical security challenges to motivate further exploration of security solutions for trusted public cloud environments. There are many problems with cloud computing in data security, one of the biggest problems in adopting data from the cloud. Since the storage takes place on the cloud service provider's servers, it poses security concerns. This means less control over stored data. Therefore, several applications are used in this document, including computational outsourcing security, access control, data service outsourcing security, multi-tenancy security and privacy, and security overhead. Security and privacy are fundamental obstacles to the success of cloud computing [5].

3. Proposed System

Nowadays cloud computing is the best thing for storing and securing data . In Our system huge numbers of these issues are because of an absence of direct control by owner and user over the innovation that serves them. Using Registration form user register in a system to login, Select file for uploading into a cloud (Private/ Public) encrypt file using AES Check Authority Permission for uploading a file or not. If authority given permission to user for uploading then enters the encryption key which is sent by authority and upload a file on selected cloud data owner can download his own file without authority permission. If user is not data owner and he want to download the other user uploaded file then he must be give the authority permission first. If authority given permission to user for downloading the file, then user enters the decryption key which is sent by authority and download a file (Here we use AES Decryption Technique). User also checks the server or cloud is misbehaved with his uploaded file or not. Every time after logout the user account password will change using random password generation technique. In our proposed system User and Cloud Service Provider is the main important concept.

4. Conclusion

In this paper, a new secure cloud system is presented. We have used encryption techniques and applied strong security against the attacker. We have used AES for encryption and decryption, which generates a random password for system security and SHA512 for key generation and authentication. In our attack mitigation, we check the attack on file and find the location of errors. No one can get access without the permission of the authority. The proposed system is faster, efficient as compared to the previous work.

References

[1] Xue, K., Chen, W., Li, W., Hong, J., & Hong, P. (2018). Combining data owner-side and cloud-side access control for encrypted cloud storage. *IEEE Transactions on Information Forensics and Security*, *13*(8), 2062-2074

[2] Sivasakthi, T., & Prabakaran, D. N. (2014). Applying Digital signature with Encryption Algorithm of user Authentication for Data Security in cloud computing. *International Journal of Innovative Research in Computer and Communication Engineering*, *2*(2), 456-459.

[3] Li, W., Xue, K., Xue, Y., & Hong, J. (2015). TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage. *IEEE Transactions on parallel and distributed systems*, *27*(5), 1484-1496.

[4] Somani, Gaurav, Manoj Singh Gaur, and Dheeraj Sanghi. "DDoS/EDoS attack in cloud: affecting everyone out there!" Proceedings of the 8th International Conference on Security of Information and Networks. ACM, 2015.

[5] Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet computing*, *16*(1), 69-73.

[6] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), 7-18.

[7] Zhou, L., Zhu, Y., & Castiglione, A. (2017). Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner. *Computers & Security*, *69*, 84-96.

[8] Hu, S., Wang, Q., Wang, J., Qin, Z., & Ren, K. (2016). Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data. *IEEE Transactions on Image Processing*, *25*(7), 3411-3425

[9] Sun, H. M., Chen, Y. H., & Lin, Y. H. (2011). oPass: A user authentication protocol resistant to password stealing and password reuse attacks. *IEEE transactions on information forensics and security*, *7*(2), 651-663.

[10] Waters, B. (2011, March). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *International workshop on public key cryptography* (pp. 53-70). Springer, Berlin, Heidelberg.