INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of Second International Conference on Science and Technology (ICOST 2021)

Proxy-Oriented Multiple File Uploading and Integrity Checking of files in Multi-Cloud Environment

Toomula Srilatha
Assistant Professor, Department of Computer Science, R.B.V.R.R Women's College, (Autonomous), Narayanaguda, Hyderabad
Toomula.srilatha@gmail.com

Abstract

Cloud servers have become an option for the organizations to store their files and data. Security in the hybrid and multi-cloud environment is always a challenge to be considered. Client can access the cloud servers to upload the files and documents. In a particular time, when cloud servers restrict access to client for storing the files, then the client can assign its proxy to process the files and upload them. Contrarily, integrity checking is also a significant security issue. It allows customers to verify if their outsourced data is kept intact without the entire data being downloaded. In Hybrid and Multi Cloud environments, a new proxy-oriented multiple file uploading and integrity checking model is proposed to resolve security problems. This concrete safety protocol is built with the aid in the Multi-Cloud Environment.

Keywords:Cloud Servers, Security, Hybrid Cloud, Multi Cloud

1. Introduction

Security is a critical factor to be considered and it is an essential factor in the Cloud environment. The area includes all processes and procedures that protect computer-based software, data and resources from accidental or unwanted entry, modification or damage. Defence against unplanned incidents and even natural disasters often require protection. Protection can be described as techniques to ensure that no individuals can read or compromise data stored in a computer without authorization. Secure computing is needed factor in ongoing cloud services. Most of the computer security measures involve data encryption and passwords.

1.1 Benefits of secure computing:

- Protecting our archives and documents
- Protects the reputation of users
- Protects the credibility of the user
- Protecting group purchases
- Protects investments from organizations

2. Literature Survey

Secure computing [1]in the cloud is the need of the hour in today's business world. The concept of security is playing a very important role in cloud computing. A large volume of storage is outsourced by the data controllers of separate companies to the cloud. Cloud adoption has motivated companies to leverage large-scale computing tools and save money. The confidential data should be encrypted by the owner prior to outsourcing to maintain data protection, which allows the conventional and powerful plaintext keyword search methodology point-less. A [1] realistic, effective, and scalable searchable encryption method is proposed that supports both ranking search for multi-keywords and concurrent search. Vector Space Model (VSM) is used to construct the searchable index to generate correct search results in order to facilitate multi-keyword search and result relevance ranking. In cloud storage [2], data security approaches like data

confidentiality, integrity and data availability have become widely significant in many software products and Applications for commercial purposes. In order to protect data privacy, several proven data possession (PDP) systems have recently been proposed. An effective, mutually verifiable, known data ownership mechanism that utilizes the shared key of Diffie-Hellman to create the homomorphic authenticator. A new form of digital proxy signature is introduced in this document [3][4]. The proxy signature enables a named party to sign on behalf of an original signer, called a proxy signer. From the point of view of the degree of delegation, the classification of proxy signatures is seen and the conditions of the proposed proxy signature are explained for partial delegation. The proxy signature scheme proposed is based on the issue of discrete logarithms. A proxy signature scheme [5-10] is a system that enables an original signer, called a proxy signer, to transfer his signing authority to a specified entity. The majority of proxy signature schemes are based on the issue of discrete logarithms. Proxy signature scheme and Weil pairing's threshold proxy signature scheme have the security evidence.[11-19]

3. Proposed System

❖ The study findings of proxy cryptography, public key cryptography and cloud authentication, file and data integrity are based on this article.

❖ The files from the user or clients can upload to multiple clouds through Proxy-oriented file uploading and assurance of data integrity.

❖ The proposed protection mechanism is successful by using public key encryption and decryption scheme, so certificate administration is excluded. Proxy-Oriented Multiple File Uploading and Integrity Checking of files in Multi-Cloud Environment is a different approach in the multi-cloud.

❖ The systematic model and security protocol of the system is efficient in generating the signatures and public keys to the mail ids of the corresponding clients. The first concrete safety protocol is intended on the basis of bilinear pairings.

❖ The developed proxy-based protection protocol is demonstrably safe in the random prophecy paradigm. The protocol will perform private screening, delegated checking and public checking depending on the original client's authorization.

❖ This protocol is used for secure multi cloud data upload and storage facilities. And aggregate signatures technique will come to practical.

❖ Integrity checking of multiple files with signature generation or hash generation will be considered securely.

❖ The key generator algorithm will send the public keys to the authenticate mail of the client

❖ The below figure depicts system architecture diagram.[20-26]

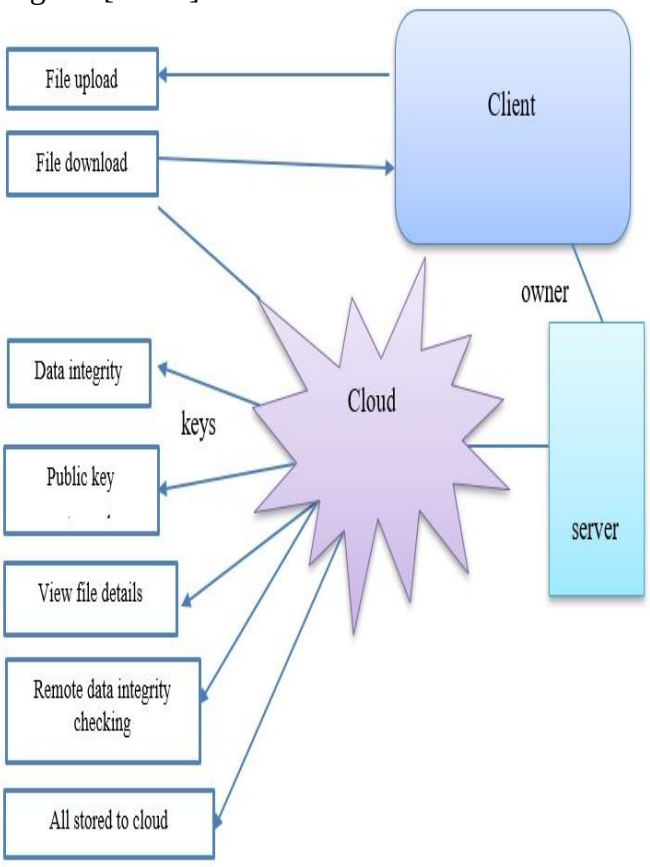

Fig. 1.System Architecture

4. Results

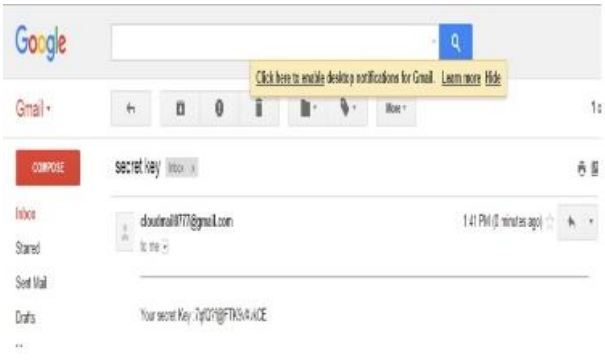

Fig 2: Secret Key to the Mail

Fig.3.To Download Files

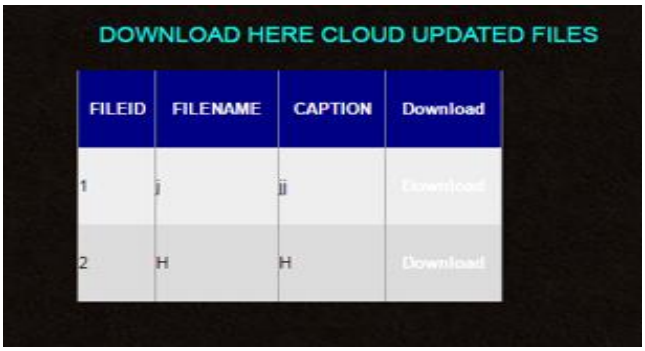

Fig. 4.Integrity Key Generated Report

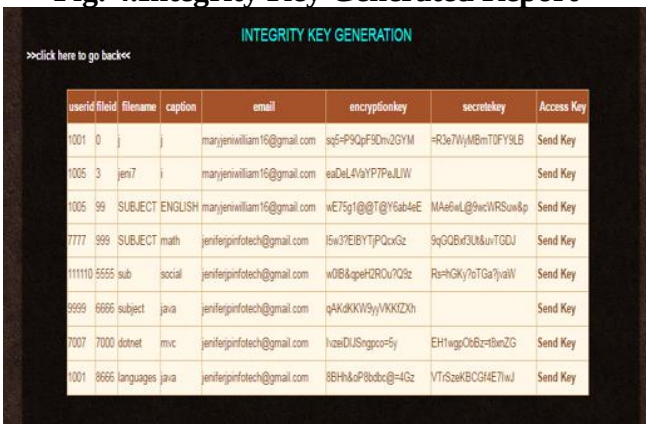

Fig.5.Report of Cloud Updated Files

Conclusions

Secure computing in the cloud has become a crucial factor for the success of many public cloud service providers. Many commercial software products and applications going for cloud storage are listing this factor as a crucial thing to be considered for the security of their files and storage. This paper proposes the security concept of uploading multiple files into proxy-server in the multi-cloud environment. By using systematic protection facts and performance review, the concrete security protocol is proved to be effective and reliable. On the other hand, file integrity checking, delegated date integrity checking, and multi-cloud integrity checking can also be done depending on the authority of the initial customer.

References

Journals

[1]. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, (2015) "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98-B, no. 1, pp. 190–200.

[2]. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, (2015) "Mutual verifiable provable data auditing in public cloud storage," J. Internet Technol., vol. 16, no. 2, pp. 317–323.

[3]. M. Mambo, K. Usuda, and E. Okamoto (1996), "Proxy signatures for delegating signing operation," in Proc. CCS, pp. 48–57.

[4]. E.-J. Yoon, Y. Choi, and C. Kim, (2013) "New ID-based proxy signature scheme with message recovery," in Grid and Pervasive Computing,vol. 7861. Berlin, Germany: Springer- Verlag, pp. 945–951.

[5]. B.-C. Chen and H.-T.Yeh,(2013) "Secure proxy signature schemes from the weil pairing," J. Supercomput., vol. 65, no. 2, pp. 496–506, 2013.

[6]. X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li,(2013) "Personal health records integrity verification using attribute-based proxy signature in cloud computing," in Internet and Distributed Computing Systems,vol. 8223. Berlin, Germany: Springer-Verlag, pp. 238–251.

[7]. H. Guo, Z. Zhang, and J. Zhang,(2014) "Proxy re-encryption with unforgeable re-encryption keys," in Cryptology and Network Security vol. 8813. Berlin, Germany: Springer-Verlag, 2014, pp. 20–33.

[8]. P. Xu, H. Chen, D. Zou, and H. Jin, (2014) "Fine-grained and heterogeneous proxy re-encryption for secure cloud storage," Chin. Sci. Bull., vol. 59, no. 32, pp. 4201–4209.

[9]. E. Zhou and Z. Li, (2014) "An improved remote data possession checking protocol in cloud storage," in Algorithms and Architectures for Parallel Processing.vol. 8631. Berlin, Germany: Springer-Verlag, pp. 611–617.

[10]. H. Wang, (2013) "Proxy provable data

possession in public clouds," IEEE Trans. Services Comput., vol. 6, no. 4, pp. 551–559.
[11].H. Wang, (2015) "Identity-based distributed provable data possession in multicloud storage," IEEE Trans. Services Comput., vol. 8, no. 2, pp. 328–340.
[12].H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, (2014) "FRR: Fair remote retrieval of outsourced private medical records in electronic health networks," J. Biomed. Inform., vol. 50, pp. 226–233.
[13].J. Zhang, W. Tang, and J. Mao, (2014) "Efficient public verification proof of retrievability scheme in cloud," Cluster Comput., vol. 17, no. 4, pp. 1401–141.
[14].J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, (2015) "A novel routing protocol providing good transmission reliability in underwater sensor networks," J. Internet Technol., vol. 16, no. 1, pp. 171–178.
[15].T. Ma et al.(2015), "Social network and tag sources based augmenting collaborative recommender system," IEICE Trans. Inf. Syst., vol. E98-D, no. 4, pp. 902–910.
[16].Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, (2011) "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859.
[17].C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, (2012) "Toward secure and dependable storage services in cloud computing," IEEE Trans. Services Comput., vol. 5, no. 2, pp. 220–232.

Conference Proceedings

[18].S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura, "Re-encryption verifiability: How to detect malicious activities of a proxy in proxy re-encryption," in Proceedings. CT-RSA Conf., vol. 9048. (2015), pp. 410–428.
[19].G. Atenieseet al., "Provable data possession at untrusted stores," in Proc. CCS, (2007), pp. 598–609.
[20].G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings. SecureComm, (2008), Art. ID 9.
[21].C. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings. CCS, (2009), pp. 213–222.
[22].H. Shacham and B. Waters, "Compact proofs of retrievability," in Proceedings. ASIACRYPT, vol. 5350. (2008), pp. 90–107.
[23].Q. Zheng and S. Xu, "Fair and dynamic proofs of retrievability," in Proceedings. CODASPY, (2011), pp. 237–248.
[24].D. Cash, A. Küpçü, and D. Wichs, "Dynamic proofs of retrievability via oblivious RAM," in Proceedings EUROCRYPT, vol. 7881. (2013), pp. 279–295.
[25].K. Huang, J. Liu, M. Xian, H. Wang, and S. Fu, "Enabling dynamic proof of retrievability in regenerating-coding-based cloud storage," in Proceedings. IEEE ICC, June(2014), pp. 712–717.
[26].C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings. IEEE INFOCOM, March (2010), pp. 1–9.