ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

Multi User Resource Sharing for Multiple Clusters in Cloud Computing

J. Krishnaveni [1], E.Gayatri [2]

M.Tech Student, Department of Computer Science Engineering, Sree Rama Engineering College, Tirupati, A.P, India[1]

Assistant Professor, Department of Computer Science Engineering, Sree Rama Engineering College, Tirupati, A.P, India[2]

ABSTRACT: In present process clear up the more than one useful resource procurement crisis in hybrid clouds. Cloud customers post their standards, and in flip vendors post bids containing rate, QoS and their supplied units of resources. The technique is scalable, which is vital on account that there are a giant number of cloud companies, with extra consistently appearing. On this paper, we endorse a secure multiowner knowledge sharing scheme, named Mona, for dynamic businesses in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share knowledge with others. Meanwhile, the storage overhead and encryption computation price of our scheme are unbiased with the quantity of revoked customers.

KEYWORDS: Cloud computing, data sharing, privacy-preserving, access control, dynamic groups.

I. INTRODUCTION

Cloud computing is a latest paradigm for providing offerings over the web. Presently, there are tons of businesses like Amazon, salesforce.Com, 3Tera, and many others. That furnishes cloud services. These cloud carriers in most cases follow a constant pricing method. Keep in mind for illustration a man or woman who desires to make use of a carrier within the type of computing platform (PaaS) on a cloud. There are cloud carriers who furnish items of that utility at unique fees, and with more than a few first-rate-of-provider (QoS) parameters. The cloud consumer is charged based on the utilization however now not on the worth derived from the supplier. This strategy has its own boundaries; for instance, it are not able to provide the first-rate offerings for the reason that the significant numbers of cloud vendors who're to be had to provide offerings in terms of a exact sort of useful resource.

Cloud computing is well-known instead to average understanding technological know-how since of its intrinsic valuable resource-sharing and low-protection qualities.

In cloud computing, the cloud carrier vendors (CSPs), similar to Amazon, are ready to provide particularly plenty of offerings to cloud users with the aid of powerful datacenters. Via migrating the nearby knowledge management systems into cloud servers, users can experience high-pleasant services and store enormous investments on their regional infrastructures. More often than not essentially the most foremost offerings offered with the aid of utilizing cloud vendors is information storage. Permit us to remember a wise information application.

A manufacturer makes it feasible for its staffs within the identical group of workers or division to retailer and share records inside the cloud. With the help of utilizing the cloud, the staffs will also be obviously released from the troublesome neighborhood knowledge storage and preservation. Nonetheless, it additionally poses a huge chance to the confidentiality of those saved files. In detailed, the cloud servers managed by the use of cloud providers should not utterly relied on by way of users whilst the info documents saved inside the cloud could also be touchy and exclusive, equivalent to trade plans. To continue know-how privateness, a traditional answer is to encrypt understanding records, after which upload the encrypted knowledge into the cloud. Lamentably, designing an effective and relaxed understanding sharing scheme for Organizations inside the cloud simply is not an effortless project due to the fact that of the following tricky disorders.

First, identification privateness is among the most gigantic limitations for the colossal deployment of cloud computing. Without the assurance of identity privateness, customers is also unwilling to become a member of in cloud computing techniques due to the fact that their precise identities would be quite simply disclosed to cloud providers and attackers. However, unconditional identification privateness may incur the abuse of privateness.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

Second, it's vastly stimulated that any member in a bunch must be in a position to absolutely enjoy the abilities storing and sharing services furnished by the use of the cloud, which is defined as the a couple of-owner system. When put next with the only-proprietor process, where quality the workforce supervisor can retailer and alter capabilities in the cloud, the few-proprietor method is bendier in realistic functions.

Final nevertheless no longer least, corporations are most generally dynamic in observe, e.g., new staff participation and current employee revocation in a organization. The alterations of membership make relaxed data sharing vastly tricky. On one hand, the anonymous process challenges new granted customers to be taught the content of capabilities records stored previous than their participation, seeing that it's unattainable for brand spanking new granted patrons to contact with nameless expertise property owners, and receive the corresponding decryption keys. On the other hand, an effective membership revocation mechanism without updating the secret keys of the rest buyers will also be appreciated to scale down the complexity of key administration.

Our contributions. To relief the challenges provided above, we recommend Mona, a comfortable multi-proprietor data sharing scheme for dynamic businesses inside the cloud. The predominant contributions of this paper incorporate:

1. We suggest a cozy multi-proprietor data sharing scheme. It implies that any purchaser inside the personnel can securely share know-how with others by way of utilizing the untrusted cloud.
2. Our proposed scheme is capable to help dynamic organizations effectually. Most likely, new granted shoppers can straight decrypt capabilities documents uploaded earlier than their participation without contacting with understanding householders. User revocation may also be really readily entire through a novel revocation record with no updating the secret keys of the rest shoppers. The size and computation overhead of encryption are average and independent with the quantity of revoked customers.
3. We furnish comfortable and privateness-preserving entry manipulate to buyers, which guarantees any member in a group to anonymously make use of the cloud useful resource. Additionally, the actual identities of knowledge homeowners may also be printed via the workforce supervisor when disputes occur.
4. We furnish rigorous safety evaluation, and participate in wide simulations to demonstrate the efficiency of our scheme in phrases of storage and computation overhead

II. SYSTEM MODEL AND DESIGN GOALS

A. SYSTEM MODEL

We don't forget a cloud computing structure with the aid of combining with an instance that a corporation uses a cloud to permit its staffs in the identical crew or department to share documents. The approach mannequin includes three exclusive entities: the cloud, a group supervisor (i.e., the enterprise supervisor), and a giant quantity of staff members (i.e., the staffs) as illustrated in Fig. 1.

Fig. 1. System model.

Cloud is operated by using CSPs and presents priced plentiful storage offerings. However, the cloud is just not entirely trusted through users when you consider that the CSPs are in all likelihood to be outside of the cloud users trusted area. Similar to, we expect that the cloud server is honest however curious. That is, the cloud server won't maliciously delete or modify user knowledge as a result of the defense of data auditing schemes, but will try to gain knowledge of the content material of the saved data and the identities of cloud users. Crew manager takes charge of method parameters new release, person registration, user revocation, and revealing the true identification of a dispute information proprietor. Within the given example, the crew manager is acted via the administrator of the company. Therefore, we anticipate that the staff manager is thoroughly relied on with the aid of the opposite parties. Staff contributors are a collection of registered users with a view to store their private knowledge into the cloud server and share them with others in the group. In our illustration, the staffs play the function of group contributors. Notice that, the team membership is dynamically converted, due to the staff resignation and new worker participation within the enterprise.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

B. DESIGN GOALS

In this section, we describe the most important design objectives of the proposed scheme including access control, data confidentiality, anonymity and traceability, and efficiency as follows:

Entry manipulate: The requirement of entry manipulate is twofold. First, staff individuals are equipped to use the cloud resource for data operations. Second, unauthorized users can't entry the cloud useful resource at any time, and revoked customers will be incapable of using the cloud once more once they are revoked.

Data confidentiality: knowledge confidentiality requires that unauthorized users together with the cloud are incapable of finding out the content material of the stored knowledge. An essential and difficult drawback for information confidentiality is to keep its availability for dynamic corporations.

Anonymity and traceability: Anonymity ensures that staff contributors can access the cloud without revealing the actual identification. Despite the fact that anonymity represents a robust security for user identification, it also poses a potential inside of attack threat to the procedure.

Effectively: The efficiency is outlined as follows: Any crew member can store and share information documents with others within the workforce by the cloud. User revocation can be completed without involving the rest users.

III. THE PROPOSED SCHEME

A. OVERVIEW

To obtain comfortable knowledge sharing for dynamic groups within the cloud, we anticipate to mix the crew signature and dynamic broadcast encryption approaches. Chiefly, the group signature scheme makes it possible for customers to anonymously use the cloud assets, and the dynamic broadcast encryption method permits data owners to safely share their information records with others including new becoming a member of customers. Unfortunately, each person has to compute revocation parameters to guard the confidentiality from the revoked users within the dynamic broadcast encryption scheme, which outcome in that each the computation overhead of the encryption and the size of the cipher text broaden with the number of revoked users. For this reason, the heavy overhead and large cipher text dimension could prevent the adoption of the published encryption scheme to capability-constrained customers. To deal with this difficult obstacle, we let the team supervisor compute the revocation parameters and make the effect public to be had via migrating them into the cloud. This kind of design can tremendously scale back the computation overhead of customers to encrypt records and the cipher text measurement. Mainly, the computation overhead of users for encryption operations and the ciphertext size is steady and impartial of the revocation customers.

IV. PERFORMANCE EVALUATIONS

In this section, we first analyze the storage cost of Mona, and then perform experiments to test its computation cost.

A. STORAGE

Without loss of generality, we set q ¼ 160 and the elements in G1 and G2 to be 161 and 1,024 bit, respectively. In addition, we assume the size of the data identity is 16 bits, which yield a group capacity of 2^{16} data files. Similarly, the size of user and group identity are also set as 16 bits.

Group manager. In Mona, the master private key of the group manager is $(G, \gamma, \xi_1, \xi_2) \in G_1 \times {Z_q}^3$, additionally, the user list and the shared data list should be stored at the group manager. Considering an actual system with 200 users and assuming that each user share 50 files in average, the total storage of the group manager is (80.125 + 42.125 *200 +2*10,000)10^{-3} ≈ 28.5 Kbytes, which is very acceptable.

Group members. Essentially, each user in our scheme only needs to store its private key $(A_i, B_i, x_i) \in {G_1}^2 \times Z_q$ which is about 60 bytes. It is worth noting that there is a tradeoff between the storage and the computation overhead. For example, the four pairing operations including (e(H,W), e(H,P), e(P,P), e(Ai, P))$G2^4$ can be precompiled once and stored for the group signature generation and verification. Therefore, the total storage of each user is about 572 bytes.

V. CONCLUSION

We design a secure knowledge sharing scheme, Mona, for dynamic corporations in an untrusted cloud. In Mona, a person is able to share information with others in the staff without revealing identity privateness to the cloud. Moreover, Mona supports effective user revocation and new person becoming a member of. Extra peculiarly, efficient person revocation can be finished by way of a public revocation record without updating the private keys of the rest users, and new users can straight decrypt documents saved in the cloud before their participation. Moreover, the storage overhead and the encryption computation price are consistent. Broad analyses show that our proposed scheme satisfies the desired safety requisites and guarantees efficiency as well.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 2, February 2017

National Conference on Recent Advancements in Engineering & Technology and Management 2017 (NCRAETM 2K17)

18th February 2017

Organized by

Sree Rama Engineering College (SRET), Tirupati- 517 507, India

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.
[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.
[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.
[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.
[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.
[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT),pp. 440-456, 2005.
[14] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-BasedCryptography, pp. 39-59, 2007.
[15] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.