ISSN 2320 - 2602

Volume 6 No.11, November 2017

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst016112017.pdf

Achieve Data Security In Cloud Computing

Ali Hasan Kamil[1], Qasim Abduljabbar Hamad[2]

[1] Southern Technical University, Thi Qar– Iraq
Ali.Gharaf88@Gmail.Com
[2] University Of Sumer,Thi Qar– Iraq
Qalrikabi@Gmail.Com

ABSTRACT

Security and privacy are very important issues in cloud computing, we propose a new Data sharing has never been easier with the advances of cloud computing, and an accurate analysis of the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of the data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) Setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. There are three users: creator, reader & writer. Creator receives a token from a trustee, i.e. organization after giving ID to the trustee. There was multiple of Key Distribution Centre (KDC) which can be scattered. A creator gives their token to one or more KDC's then creator receives keys for encryption & decryption and for signing from KDC's. The message is encrypted under an access policy which means it decides who can access the data stored in the cloud. Creator decides on a claim policy to prove her authenticity and signs the message under this claim. The cipher text is sent to the cloud. The cloud verifies the signature and stores the cipher text. When a reader wants to read, the cloud sends cipher text. If the user has attributes matching with access policy, it can decrypt and get back the original message.

Keywords:Cloud Computing, Security, Privacy,Encryption & Decryption.

1. INTRODUCTION

Much of the information keep in clouds is very sensible, for example, social networks stored in medical records. Thus, important problems in cloud computing. In one hand, the user ought to testify itself before beginning any group action, and on the opposite hand, it must be confirm that the cloud doesn't tamper with the information that's outsourced. User privacy is additionally needed so the cloud or different users don't grasp the identity of the user. The physical property of fast resource rating based and risk of transformation. Cloud computing is reworking the terribly nature of however businesses use information technology. This paradigm to shifting the elementary facet that information square measure being centralized or outsourced to the cloud. From users' position together with each people and IT enterprises are storing data remotely to the cloud in a very versatile on-demand manner brings appealing benefits, the global data to access the location independence and personnel maintenance. They entire data from the cloud to normal approach for checking data correctness is to retrieve and so verify information integrity by checking the correctness of signatures, in this data to check RSA algorithm to be implemented. This typical approach is ready to with success check the correctness of cloud information certainly. The potency of exploitation this ancient approach on cloud information is doubtful, the most reason is that the aspect of cloud data is massive generally. Downloading the entire cloud information to verify information integrity can price or maybe waste user's amounts of computation and communication resources, particularly once data are corrupted within the cloud. Besides, several uses of cloud data don't essentially would like users to transfer the entire cloud data to local devices. It's as a result of cloud suppliers, appreciate Amazon, can give users computation services directly on large-scale information that already existed within the cloud.

This mechanism to check integrity in public verifier without downloading the shared information from cloud, it is referred to the public audit. Information is divided into many small blocks, in entire block should be independently signed by the owner and entire blocks alternatively a random combination, integrity checking of all the retrieved data. If public verifier would like to expend the owner data from the cloud or third party audit. Who should be providing authority for integrity checking services.

Therefore Alice and Bob work along as a group and file sharing in the cloud. They divided into a number of small blocks in a shared file, in each and entire block is separately signed by two users with the existing public audit in the cloud. User should be modified in block shared file at only once, they user need private key to sign the new block. Ultimately, different user signed by a different blocks are modified by two different users. Then entire data check in order to correctly audit integrity, a public verifier chooses the proper public key to the entire block.

In Existing system is leakage of identity, privacy in public verifiers, to introduce a new notable privacy issue in shared data. They protect the secret information, it's crucial and disapprove to preserve the identify privacy from public verifiers in public audit. The shared data to solve the identity privacy.

2. RELATED WORK

S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," [1]

They proposed a brand new privacy conserving attested access management theme for securing information in clouds. Within the projected theme, the cloud verifies the credibleness of the user while not knowing the user's identity before storing info. Our theme additionally has the other feature of access management during which solely valid users are able to decipher the hold on info. The theme prevents replay attacks and supports creation, modification, and reading information hold on within the cloud. Moreover, our authentication and access management theme is localized and sturdy, not like alternative access management schemes designed for clouds that are centralized. The communication, computation, and storage overheads are like centralized approaches.

J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," [2]

With the recent important development within the transportable device market, cloud computing is obtaining additional and additional used. Several sensitive knowledge areheld on in cloud central servers. To confirm privacy, this knowledge is typically encrypted before being uploaded—making file looking sophisticated. Though previous cloud computing searchable secret writing schemes permit users to look encrypted knowledge by keywords firmly, these techniques solely support precise keyword search, and can fail if there are some orthography errors or if some morphological variants of words are used. During this paper, They offer the answer for fuzzy keyword search over encrypted cloud knowledge. K-grams are employed to supply fuzzy results. For security reasons, we tend to use 2 separate servers that can't communicate with one another. Theirexperimental result shows that their system is effective and ascendable to handle sizable amount of encrypted files.

S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," [3]

Ciphertext-Policy Attribute primarily based cryptography (CP-ABE) may be a promising scientific discipline primitive for fine-grained access management of shared knowledge. In CP-ABE, every user is related to a collection of attributes and knowledge are encrypted with access structures on attributes. A user is in a position to decode a ciphertext if and on condition that his attributes satisfy the ciphertext access structure. Beside this basic property, sensible applications sometimes produce other needs. During this paper, they tend to concentrate on a vital issue of attribute revocation that is cumbersome for CP-ABE schemes. Especially, they tend to resolve this difficult issue by considering a lot of sensible eventualities within which semi-trustable on-line proxy servers are out there. As compared to existing schemes, our projected answer allows the authority to revoke user attributes with nominal effort. They tend to win this by unambiguously desegregation the technique of proxy re-encryption with CP-ABE, and modify the authority to delegate most of effortful tasks to proxy servers. Formal analysis shows that our projected theme is incontrovertibly secure against chosen ciphertext attacks. Additionally, they tend to show that our technique may be applicable to the Key-Policy Attribute primarily based cryptography (KP-ABE) counterpart.

3. EXISTING SYSTEM

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse.

Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owners anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality.

A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not perfectly happy with trusting the security of the VM or the honesty of the technical staff.

DISADVANTAGES

- correctness of the data in the cloud is being put at risk
- The costs and complexities involved generally increase with the number of the decryption keys to be shared.

4. PROPOSED SYSTEM

In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size. Specifically, our problem statement is “To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the ciphertexts (produced by the encryption scheme) is decryptable by a constant-size decryption key (generated by the owner of the master-secret key).” We solve this problem by introducing a special type of public-key encryption which we call key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of the ciphertext called class. That means the ciphertexts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.

ADVANTAGES

- The extracted key have can be an aggregate key which is as compact as a secret key for a single class.
- The delegation of decryption can be efficiently implemented with the aggregate key.
- Storage correctness
- Privacy preserving

5. ARCHITECTURE DIAGRAM

The System Architecture involves of three Parties: User, Cloud Server and KDC(Key Distribution Centre) as illustrated in figure 1.

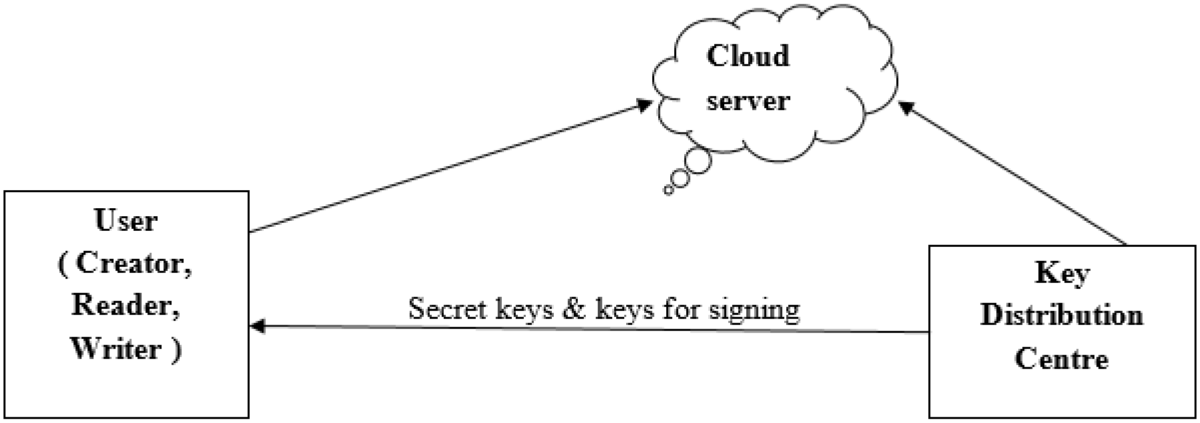
Cloud server
User (Creator, Reader, Writer)
Secret keys & keys for signing
Key Distribution Centre

Figure 1: System Architecture

The user is the person who is allowed to access and using the cloud. The user divided into (Creator, Reader and Writer). The Creator have all the privileges (create, read and write) in his own file. The Reader can see the file and can’t change anything. The Writer has privileges to modify the file. Cloud Server is a virtual server that can manage the resources in the cloud computing. Key Distribution Centre (KDC) is responsible for sharing keys between users in the network and manage privileges of users to reach for some services.

6. MODULES

6.1 User Registration and Control:

In this module, every user's give their personal details for registration process. After registration every user will get an ID for accessing the cloud space. If any of the user wants to edit their information they have submit the details to the admin after that the admin will do the edit and update information process. Every user will receive an ID by the email as already has submitted it in this module [1][3].

6.2 Sharing Information's

In this module, every user's share their information and data's in their own cloud space provided by the admin. That information may be sensitive or important data's. For providing security for their information every user's storing the information in their specific cloud. Registered users only can store the data in the cloud. The owner of the file can determine who can access his file in the cloud [2][3][12].

6.3 Encryption Process

In this module, the information and data's shared by the user in the cloud is encrypted by using RSA algorithm. All of the information shared by every user is encrypted and stored in the cloud [5][11].

6.4 Integrity Checking

Integrity checking is the process of comparing the encrypted information with altered cipher text. If there is any change in detection a message, will send to the user that the encryption process is not done properly. If there is no change in detection means, then it will allow doing the next process. Integrity checking is mainly used for anti-malware controls [4] [6].

6.5 Data Forwarding

In this module, the encrypted data or information stored in the cloud is forwarded to another user account by using that user's public key. If any user wants to share their information with their friends or someone they can directly forward the encrypted data to them. Without downloading the data, the user can forward the information to another user[7] [10].

6.6 Data Extraction

In this module, the encrypted data is decrypted by the user using the public key of the owner of the data. Decryption is the process of converting cipher text into plain text. The RSA algorithm is used for encrypting and decrypting the information. The user can view the data and also can download the data with high security [8] [9].

7. CONCLUSION

Cloud Computing is a technology that allows users to share data and applications over the internet. Cloud computing consists of shared computing resources that are accessed as a service. The computing resources are aggregate of available hardware and software computer. Most of the IT organizations are preparing themselves to migrating to cloud computing. We suggested this system for the cloud computing users to help themandkeep theirfiles safe in cloud computing for sharing them with other users over the internet.In our system we supported the privacy of the users in cloud computing.

REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[2] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445,2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270,2010.

[4] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[5] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[7] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[8] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[9] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[10] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[11]. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.

[12]. R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.