ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 8, August 2017

Attribute-Based Hierarchy Level Storage Supporting Secure Deduplication of Encrypted Data in Cloud

S. Dhivya[a], M.Sc. (IT) and R. Banumathi[b], M.Phil. , M.Tech. (CSE)
[a]Research Scholar, Department of Computer Science, PRIST University, Thanjavur.
[b]Research Supervisor, Department of Computer Science, PRIST University, Thanjavur.

Abstract: Meanwhile, cloud computing is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Access control is paramount as it is the first line of defense that prevents unauthorized access to the shared data. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to- end data confidentiality assurance in the cloud and beyond. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying cipher text-policy, making the computation over encrypted data a very hard problem. The proposed scheme not only achieves scalability due to its hierarchical structure.

Keywords: Private Key, Chipper text, Hierarchical Structure, Bandwidth, Encryption, CP-ABE (CKM-CP-ABE).

I. INTRODUCTION

In cloud computing, authority accepts the user enrollment and creates some parameters. Cloud service provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated ciphertext to CSP. User downloads and decrypts the interested ciphertext from CSP. The shared files usually have hierarchical structure. That is, departments of files are divided into a number of hierarchy sub departments located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of ciphertext and time cost of encryption could be saved. Presently a day's more number of plans utilized encryption for control the information in Cloud. It empowers clients with restricted computational assets to outsource their expansive calculation workloads to the cloud, and monetarily appreciate the monstrous computational power, data transfer capacity, stockpiling, and even proper programming that can be partaken in a compensation for each utilization way.

To realize scalable, flexible and fine-grained access control of outsourced data in cloud computing. The outsourced computation workloads contain sensitive information such as business financial records, proprietary research data or personally identifiable health records etc. Users may try to access the data files outside their privileges. Hence a hierarchy is proposed where a particular department of users trusts a domain authority. The domain authority in turn trusts the trusted authority.

We provide the privacy secure in public social cloud computing. In our project we implement hierarchical attribute base security the hierarchy are Cloud authority, Domain authority and users. Cloud authority can only have privilege to create or remove the domain(private cloud authority) in cloud and they can maintain all the details in overall cloud Domain authority can create or remove the users inside the domain this users are called private users . Users are two types private cloud user and public cloud user's Private cloud users are depends the domain Public users under cloud authority. Users can upload the files in two ways: Public and Private. If the private user upload the public file, the file visibility and accessibility is only within domain itself and same domain users can access that file without any security authentication If the public user upload the public file, the file visibility and accessibility is

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 8, August 2017

always public any cloud user can access that file . For Private upload If private user upload the private file means that file visibility is only within domain but file accessibility is who have the secrete key (OTP) means who have privilege to access the file If the public user upload the private file means that file visibility is public anyone can visible the file but who have a privilege (OTP) to access they only can access the file.

II. Related Work

Distributed computing is a progressive registering worldview which empowers adaptable, on-request and minimal effort utilization of figuring assets. Those points of interest, unexpectedly, are the reasons for security and protection issues, which rise in light of the fact that the information claimed by various clients are put away in some cloud servers rather than under their own control. The security issue of distributed computing is yet to be settled. To manage security issues, different plans in light of the Attribute-Based Encryption have been utilized. From one perspective, the outsourced figuring workloads often contain sensitive information, for instance, the business money related records, prohibitive research data, or eventually identifiable prosperity information et cetera. To fight against unapproved information spillage, sensitive data must be mixed before outsourcing so as to offer end to-end data protection affirmation in the cloud and past. Regardless, normal data encryption procedures by and large shield cloud from playing out any critical operation of the essential figure content game plan, making the count over encoded data a troublesome issue. The proposed plot not simply achieves flexibility due to its dynamic structure. We give the protection secure out in the open social distributed computing. In our venture we actualize progressive property base security the pecking orders are Cloud specialist, Domain expert and clients. Cloud expert can just have benefit to make or expel the domain (private cloud specialist) in cloud and they can keep up every one of the points of interest in general cloud Domain expert can make or evacuate the clients inside the area this clients are called private clients. Clients are two sorts private cloud client and open cloud client's Private cloud clients are depends the space Public clients under cloud specialist. Clients can transfer the documents in two ways: Public and Private. On the off chance that the private client transfer general society document, the record perceivability and availability is just inside area itself and same space clients can get to that document with no security validation If the general population client transfer people in general document, the record perceivability and openness is constantly open any cloud client can get to that document. For Private transfer If private client transfer the private document implies that record perceivability is just inside space yet document openness is who have the emit key (OTP) implies who have benefit to get to the record If general society client transfer the private document implies that document perceivability is open anybody can obvious the document yet who have a benefit (OTP) to get to they just can get to the document.

III. System Analysis

3.1 Problem Statement

Existing system can't secure computation outsourcing data. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing. Ordinary data encryption techniques can't secure cloud underlying plaintext data. Making the computation over encrypted data a very hard problem. Complex of access control policies. Cipher-texts are not encrypted to one particular user as in traditional public key cryptography. Assigning multiple values to the same attribute.

3.2 Existing System

- The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military.
- The hierarchy structure of shared files hasn't been explored in CP-ABE. Using Cipher text-policy attribute based encryption to secure the cloud storage part.
- The authority for file access control in which authorized of all operations on cloud data can be managed in the entire manner.
- To avoid unauthorized information leakage, sensitive data have to be encrypted before outsourcing. Role based encryption is used for encrypting the data based on the authority provided.

3.3 Proposed System

- We offer the security of social cloud computing. In this paper we put into practice hierarchical security, Cloud authority, Domain authority and users. Cloud authority can only have a privilege to create or remove the province in cloud and they can preserve all the details in overall cloud Domain authority can create or eliminate the users contained by the domain this users are called private users .

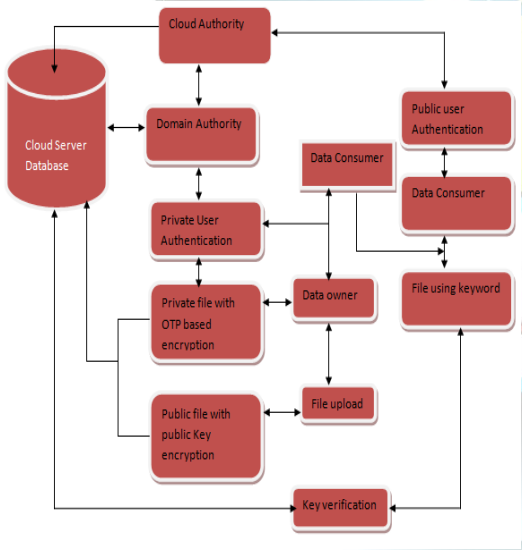
All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 8, August 2017

- Two type users will be there. One is private cloud user and another one is public cloud users. Private users are rely on the domain, Public users under cloud authority. User has a two way of uploading files Public and Private.
- If one file uploaded by private user, file visibility and convenience having only within domain without confirmation. If some file should uploaded by public user's then, file access privileges having all the users.
- If file uploading the private user means file visibility is only within field but file accessibility is who have the secrete key (OTP) means who have license to access the file If the public user upload the private file means that file visibility is public anyone can noticeable the file but who have a privilege like one time password to access they only can access the file.

IV. System Architecture



4.1 Modules

- Data Owner
- Data Consumer
- Domain level Security
- Attribute based security
- Secret file accessing

Modules Description

4.1.1 Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the encrypted data file. The data owner can set the access privilege to the encrypted data file.

4.1.2 Data Consumer

The user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Domain authority and the Data users are controlled by the Domain Authority only.

4.1.3 Domain Level Security

The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. we assume that communication channels between all parties are secured using standard security protocols.

4.1.4 Attribute Based Security

The HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. We formally proved the security of HASBE based on the security of CP-ABE. A hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. HASBE extends the cipher text-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control.

4.1.5 Secret Files Accessing

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

V. Result And Discussion

In its simplistic definition, a hybrid cloud is a combination of both public and private clouds. If we apply the definition from the National Institute of Standards and

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 8, August 2017

Technology (NIST), "a hybrid cloud is a combination of public and private clouds bound together by either standardized or proprietary technology that enables data and application portability." It could be a combination of a private cloud inside an organization with one or more public cloud providers or a private cloud hosted on third-party premises with one or more public cloud providers.

Trend Micro, a cloud security company, recently conducted a survey which indicated that public cloud services fail to meet IT and business requirements of some of the business organizations. A hybrid cloud environment can help meet their needs. In some ways, hybrid clouds can be considered an intermediate stage as enterprises prepare to move most of their workloads to public clouds.

Benefits

Hybrid clouds offer the cost and scale benefits of public clouds while also offering the security and control of private clouds. In this section, we will highlight some of the business benefits of hybrid clouds.

Public Cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

Private Cloud

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud:

On-premise Private Cloud: On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.

Externally hosted Private Cloud: This type of private cloud is hosted externally with a cloud provider, where the provider facilitates an exclusive cloud environment with full guarantee of privacy. This is best suited for enterprises that don't prefer a public cloud due to sharing of physical resources.

Data Recovery and Availability

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support.

- Appropriate clustering and Fail over
- Data Replication
- System monitoring (Transactions monitoring, logs monitoring and others) Maintenance (Runtime Governance)
- Disaster recovery Capacity and
- performance management

If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.

Management Capabilities

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto-scaling" for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

VI. CONCLUSION

A semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to $N - 2$ authority compromise, which is highly preferable especially in Internet-based cloud computing environment.

Future enhancement of this project is following schemes. A unified scheme for resource protection in automated trust negotiation. Automated trust negotiation using cryptographic credentials In prospective we will improving the performance. In future we will include the image, audio, video files also .In this system we are using limited size of files only, it will be enlarging in future work. The time cost of decryption is also decrease if the user needs to decrypt multiple files.

All Rights Reserved © 2017 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 8, August 2017

REFERENCES

[1]. M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secured duplication," in Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[2]. K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptography: Theory, practice and future research directions," Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

[3]. K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics: State-of-the-art and future directions," Digital Investigation, vol. 18, pp. 77–78, 2016.

[4]. C. Fan, S. Huang, and H. Rung, "Arbitrary-state attribute-based encryption with dynamic membership," IEEE Transactions on Computers, vol. 63, no. 8, pp. 1951–1961, August 2014.

[5]. F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, "CP-ABE with constant-size keys for lightweight devices," IEEE Transactions on Information Forensics and Security, vol. 9, no 5, pp. 763–771, May 2014.

[6]. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, pp. 1667–1680, October 2014.

[7]. D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing / Elsevier, 2014. [Online]. Available: http://www.elsevier.com/books/cloud-storageforensics/quick/978-0-12-419970-5

[8]. D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants," J. Network and Computer Applications, vol. 40, pp. 179–193, 2014.

[9]. T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "ktimes attribute-based anonymous access control for cloud computing," IEEE Transactions on Computers, vol. 64, no. 9, pp. 2595–2608, September 2015.

[10]. T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang, "Privacy preserving cloud data access with multi-authorities," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2634–2642

[11]. Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K. R. Choo, "Cloud based data sharing withfine-grained proxy re-encryption," Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

[12]. B. Zhu, K. Li, and R. H. Patterson, "Avoiding the disk bottleneck in the data domain deduplicationfile system," in 6th USENIX Conference on File and Storage Technologies, FAST 2008, February 2629, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

All Rights Reserved © 2017 IJARTET