|| Volume 2 || Issue 4 || OCTOBER 2017|| ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

A Review on - Fragmentation & Replication of Data in Cloud Storage & Security

Mr. D.G. Deshmukh
P.G. Student Department of Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, Maharashtra, India

Abstract— ***Outsourcing data to a third-party administrative control, as is done in cloud computing, gives rise to security concerns. The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures are required to protect data within the cloud. However, the employed security strategy must also take into account the optimization of the data retrieval time. In this paper, we propose Di- vision and Replication of Data in the Cloud with Attribute based encryption (ABE) that collectively approaches the security and performance issues. In this system, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. And also, This kind of computing model brings challenges to the security and privacy of data stored in cloud. Attribute-based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting. However, the computation cost and cipher text size in most ABE schemes grow with the complexity of the access policy. Outsourced ABE (OABE) with fine-grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider(CSP).***

Keywords: *attribute-based encryption; cloud computing; outsourced key-issuing; outsourced decryption; Division of Cloud Data.*

I INTRODUCTION

Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. Cloud security issues may stem due to the core technologies implementation (virtual machine (VM). The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes must be prevented. The main aim of our project is secure the files store on cloud. The division of a file into fragments is performed based on a given user criteria. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security. This system selects the nodes in a manner that they are not adjacent and are at certain distance from each other. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time.

Develop a scheme for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes. The proposed System scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. These systems do not rely on traditional cryptographic techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the data. this system ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.

From the above discussion, this system can deduce that both security and performance are critical for the next generation large-scale systems, such as clouds. Therefore, in this paper, this system collectively approach the issue of security and performance as a secure data replication problem. this system present Division and Replication of Data in the Cloud for Optimal Performance and Security that judicially fragments user files into pieces and replicates the mat strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes (this system use the term node to represent computing, storage, physical, and virtual machines) contains a distinct fragment to increase the data security. As unsuccessful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, this systems elect the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the T-coloring

Then other hand Cloud computing is a new computation model in which computing resources is regarded as service to provide computing operations. This kind of computing paradigm enables us to release computing resources

rapidly. So this system can access resource rich, various, and convenient computing resources on demand. The computing paradigm also brings some challenges to the security and privacy of data when a user outsources sensitive data to cloud servers. Many applications use complex access control mechanisms to protect encrypted sensitive information. Sahai and Waters addressed this problem by introducing the concept for ABE. This kind of new public key cryptographic primitive enables us to implement access control over encrypted files by utilizing access policies associated with cipher texts or private keys. Two types of ABE schemes, namely key-policy ABE (KPABE) and cipher text policy ABE(CP-ABE)are proposed. For KP-ABE scheme, each cipher text is related to asset of attributes, and each users private key is associated with an access policy for attributes. A user is able to decrypt a cipher text if and only if the attribute set related to the cipher text satisfies the access policy associated with the users private key. For CP-ABE scheme, the role so fan attribute set and an access policy are reversed. Be then court provided a CP-ABE scheme, which ensures encrypted data is kept confidential even if the storage server is untrusted. In order to withstand collusion attack and avoid sensitive information leakage from access structure, Qian et al. proposed a privacy preserving decentralized AB Escheme with fully hidden access structure. Deng et al. constructed a cipher text policy hierarchical attribute based encryption (CP-HABE) with short cipher texts, which enables a CP-HABE system to host many users from different organizations by delegating keys. In CPABE scheme, a malicious user may be shares his attributes with other users, which might leak his decryption privilege as a decryption black box due to financial profits.

In ABE Attribute based encryption, this system consider the case that the user Alice has a large number of data stored in the cloud. If Alice submits a request for accessing the encrypted data stored in the CSP, according to the traditional out sourced ABE scheme, the CSP downloads all the data, executes partial decryption and responses all corresponding data of Alice. This greatly increases the cost for communication and storage at Alice side. In this article, this system organically integrate outsourced ABE (OABE) with PEKS and present a novel cryptographic paradigm called outsourced attribute-based encryption scheme with keyword search function (KSF-OABE). In our system, when the user wants to outsource his sensitive information to the public cloud, he encrypts the sensitive data under an attribute set and builds indexes of keywords. As a result, the users can decrypt the cipher text only if their access policies satisfy the corresponding attributes. By this way, when Alice submits the request with a trapdoor corresponding to a keyword “current”, CSP downloads all the data intended for Alice and just returns a partial cipher text associated with the keyword “current”. Therefore, Alice can exclude the data what she does not hope to read.

II LITERATURE SURVRY

1.K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, “On the characteri- zation of the structural robustness of data center networks,” IEEE Transactions on Cloud Computing,Vol. 1, No. 1, 2013, pp. 64-77.

In this paper, Author studied the structural robustness of the state-of-the-art data center network (DCN) architectures. Our results revealed that the DCell architecture de- grades gracefully under all of the failure types as compared to the Fat Tree and Three Tier architecture. Because of the connectivity pattern, layered architecture, and heterogeneous nature of the network, the results demonstrated that the classical robustness metrics are insufficient to quantify the DCN robustness appropriately. Hence forth, signifying and igniting the need for new robustness metrics for the DCN robustness quantification. Author proposed deterioration metric to quantify the DCN robustness. The deterioration metric evaluates the network robustness based on the percentage change in the graph structure. The results of the deterioration metric illustrated that the DCell is the most robust architecture among all of the considered DCNs[2].

2 2. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, “Energy-efficient data replication in cloud computing datacenters,” In IEEE Globecom Workshops, 2013, pp. 446-451.

This paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications. The performance evaluation is carried out using Green Cloud the simulator focusing on energy efficiency and communication processes in cloud computing data centers. The obtained results confirm that replicating data closer to data consumers, i.e., cloud applications, can reduce energy consumption, bandwidth usage, and communication delays significantly [3].

3 3. K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its

use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits the security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or in extent. Author has presented security issues for cloud models : IaaS, PaaS, and SaaS, which vary depending on the model. As described in this paper, storage, virtualization, and net- works are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines[1].

4.L.M.Kaufman,"Datasecurityintheworldofcloudcomputing ,"IEEESecurityandPri- vacy, Vol. 7, No. 4, 2009, pp.61-64.

In this paper, Author elucidate cloud computing and major security issues of cloud computing. By utilizing various facilities and services provided by cloud one can in- crease performance, agility and efficiency in addition to reduce cost and management responsibilities of an enterprise. Though there are lots of advantages of cloud, there are yet numerous challenges to be faced by cloud computing such as privacy issues and data security. In this paper Author have tried to address most critical data security challenges of cloud. Many standard organizations such as National Institute of Standards and Technology (NIST), 8 Cloud Security Alliance (CSA) and Cloud Computing Interoperability Forum (CCIF) are trying to develop standard store solve various security issue so cloud. Cloud computing has the potential to provide a secure and economically viable IT solu- tion in the future[4].

5.S.Pearson,Y.ShenandM.Mowbray,"A Privacy Manager for Cloud Computing," Proc. First International Conference Cloud Computing(CloudCom09), M. Gilje-Jaatun, G. Zhaoand C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

In this paper Author describe a privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused, and also assists the cloud computing provider to conform to privacy law. Cloud computing, in which services are carried out on behalf of customers on hardware that the customers do not own or manage, is an increasingly fashionable business model. The input data for cloud services is uploaded by the user to the cloud, which means that they typically result in users data being present in unencrypted form on a machine that the user does no town or control. This poses some inherent privacy challenges[5].

6.A.Sahaiand B.Waters, "FuzzyIdentity Based Encryption, "EUROCRYPT05,LNCS, vol. 3494, pp.457-473,2005.

Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, this systems how that Fuzzy-IBE can be used for a type of application that this system term "attribute-based encryption". In this paper Author present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity- Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Addition- ally, our basic construction does not use random oracles. this system prove the security of our schemes under the Selective-ID security model[6].

7. V. Goyal, O. Pandey, A. Sahai, andB. Waters, "Attribute-Based Encryption for Fine- Grained Access Control of Encrypted Data,"Proc.13th ACM Conference on Computer and Communications Security (CCS06), pp.89- 98,2006, doi:10. 1145 /1180405.1180418.

Authors develop an crypto system for One grained sharing of encrypted data that this system call Key Policy Attribute-Based Encryption(KP-ABE).In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Author demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption [7].

8. A. Lewko, T. Okamoto, A. Sahai, K. Takashimaand B. Waters, "Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,"EUROCRYPT10, H. Gilbert, ed., LNCS 6110, Berlin: Springer-Verlag, pp. 62-91, 2010.

In this paper, Author presents two fully secure functional encryption schemes. Our first result is a fully secure attribute-based encryption (ABE) scheme. Previous constructions of ABE were only proven to be selectively secure. Author achieves full security by adapting the dual system encryption methodology recently introduced by Waters and previously leveraged to obtain fully secure IBE and HIBE systems. The primary challenge in applying dual system encryption to ABE is the richer structure of keys and cipher texts. In an IBE or HIBE system, keys and cipher texts are both associated with the same type of simple object: identities. In an ABE system, keys and cipher texts are associated with more complex objects: attributes and access formulas. Author use a novel information- the or argument to adapt the dual system encryption methodology to the more complicated structure of ABE systems. Authors construct our system in Composite order bilinear groups, where the order is a product of three primes.

Authors prove the security of our system from three static assumptions.

III CONCLUSION

The proposed System, a cloud storage security scheme that collectively deals with the security and performance in term so time. The data file was fragmented and the fragments are dispersed over multiple nodes. This system proposes a CP-ABE scheme that provides out-sourcing key-issuing, decryption and keyword search function. This proposed system will be efficient since this system only need to download the partial decryption cipher text corresponding to a specific keyword. The time-consuming pairing operation can be out sourced to the cloud service provider, while the slight operations can be done by users. Thus, the computation cost at both users and trusted authority sides will be minimized. The Division and replication of data in cloud with Attribute Based Encryption. With help of trapdoor provider work is reduces.

REFERENCES

[1]K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.

[2]K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characteri- zation of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.

[3]D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446-451. .

[4]L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[5]S. Pearson, Y. Shen and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc.First International ConferenceCloud Computing(CloudCom09), M. Gilje-Jaatun, G. Zhao and C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

[6]W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.

[7]S. Pearson, Y. Shen and M. Mowbray, "A Privacy Manager for Cloud Comput- ing,"Proc.First International Conference Cloud Computing(CloudCom'09), M. Gilje-Jaatun, G. Zhao and C. Rong, eds., LNCS 5931, Berlin: Springer-Verlag, pp. 90-106, 2009.

[8]A. Sahai and B. Waters,"Fuzzy Identity-Based Encryption,"EUROCRYPT05, LNCS, vol. 3494, pp. 457-473,2005.

[9]V. Goyal, O. Pandey, A. Sahai, andB. Waters, "Attribute Based Encryption for Fine Grained Access Control of Encrypted Data,"Proc.13thACMConferenceonComputerand Communications Security(CCS '06), pp. 89-98, 2006,doi:10.1145/1180405.1180418.

[10]A. Lewko, T. Okamoto, A. Sahai, K. Takashimaand B. Waters, "Attribute-Based Encryptionand (Hierarchical) Inner Product Encryption,"EUROCRYPT10,H.Gilbert,ed.,LNCS 6110, Berlin: Springer-Verlag, pp. 62-91,2010.