International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-5, Issue-2, March 2017
DOI: 10.21276/ijircst.2017.5.2.8

Secure Big Data Access Control Policies for Cloud Computing Environment

Taniya Jain (M.Tech Scholar), Asst. Prof. Javed Akhtar Khan

Abstract— **As the term indicates the Big data it means we are work for the something big or can say something large in the Amount, Data the high volume is known as the big data.Now a Day for storing the data file in the Computer Science Engineering we are used the Hard disk, some of the storage place , these storage device may store the data in a Giga byte capability and Terabyte capability or many more, Now a day we are used the some new technology call the cloud environment. So in this work I am study the big data storing process in the Cloud environment, big data fetching from the cloud in a securer manner. So in this dissertation work I am also include the some information about the existing work and some of the algorithm that war already proposed by the researcher in the various paper. My work is based on the Attribute-Based Encryption(ABE) is promising technique to ensure the end-to-end security of big data in the cloud However, the policy updating has always been a challenging issue when ABE is used to construct access control schemes.**

Index Terms— **ABE, Big Data, cloud, Cipher Text, Plain Text**

I. INTRODUCTION CLOUD COMPUTING

Cloud Computing refers to manipulating, accessing and configuring the applications online. It offers online data storage, infrastructure & cloud application. Cloud computing is an IT operation form, based on virtualization, where resources, in terms of infrastructure, appliance and data are deployed via the internet as a distributed service by one or some service providers[1] Data integrity Evaluation in cloud Database –as-a – service is explore the data integrity for the cloud environment . These services are scalable on require and can be valued on a pay per use basis. Cloud infrastructure provides extensive facilities for the client such as process, storage, power, networks, space and other computational possessions, so that the customer can set and perform their convention software as well as applications and operating system. Client does not supervise or organize the cloud infrastructure yet they have been in charge of on operating systems, applications, storage space and probably their collection and components with the cloud computing key technology [2] . One of the main apprehension in cloud computing is the possibility of incursion of privacy. As cloud computing is achieving augmented popularity, apprehension are being voiced about the safety issues bring in through the acceptance of this new model.description of this inventive deployment model, be different broadly from them of conventional architectures [3]a new approach using redundancy technique with improve security in cloud computing.

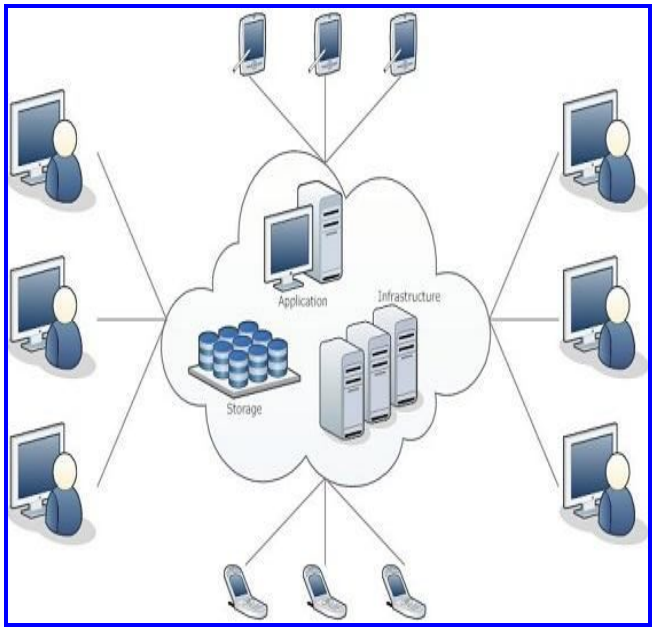

Figure 1: Cloud Computing Data Integrity [1]

. Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Most of us use cloud computing all day long without realizing it. The same applies to Web-based email. Once upon a time, email was something you could only send and receive using a program running on your PC (sometimes called a mail client). But then Web-based services such as Hotmail came along and carried email off into the cloud. Preparing documents over the Net is a newer example of cloud computing. Simply log

Manuscript received March 14, 2017
Taniya Jain (M.Tech Scholar), Asst. Prof. Javed Akhtar Khan Department of Computer Science & Engineering, Takshshila Group of Institute, INDIA

on to a web-based service such as Google Documents and you can create a document, spreadsheet, presentation, or whatever you like using Web-based software. Instead of typing your words into a program like Microsoft Word or Open Office, running on your computer, you're using similar software running on a PC at one of Google's world-wide data centers.

II CLOUD COMPUTING IMPORTANCE

Cloud Computing has several recompense. Some of them are listed below:

- One can right of entry applications as utilities, over the Internet.
- Stage-manage and configure the relevance online at any time.
- It does not necessitate installing a explicit piece of software to right to use or manipulating cloud application.
- Cloud computing propose online progress and deployment tools, programming runtime surroundings through Platform as a Service model.
- Cloud resources are accessible over the network in a method that provides platform independent right of entry to any type of clients.
- Cloud computing put forward on-demand self-service. The resources can be used lacking interaction with cloud service contributor.
- Cloud Computing is extremely cost effective since it operates at higher efficiencies with larger utilization. It just has need of an Internet connection.
- Cloud Computing offers load comparison that makes it more reliable.

III LITERATURE SURVEY

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). In this paper author develop a new cryptosystem for fine-grained sharing of encrypted data that is called Key-Policy Attribute-Based Encryption[6] (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. In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. If any server storing the data is compromised, then the confidentiality of the data will be compromised. Previous Attribute Based Encryption[7] systems used attributes to describe the encrypted data and built policies into user's keys; in this system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. This methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). In addition, Author provides an implementation of our system and give performance measurements. Fully secure functional encryption schemes: a fully secure attribute-based encryption (ABE)[4]scheme and a fully secure (attribute-hiding) predicate encryption (PE) scheme for inner-product predicates. In both cases, previous constructions were only proven to be selectively secure. Both results use novel strategies to adapt the dual system encryption methodology introduced by Waters. Author construct our ABE scheme in composite order bilinear groups, and prove its security from three static assumptions. ABE scheme supports arbitrary monotone access formulas. Predicate encryption scheme is constructed via a new approach on bilinear pairings using the notion of dual pairing vector spaces proposed by Okamoto and Takashima . A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In this system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in this system each component will come from a potentially different authority, where no coordination between such authorities. Researcher create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. In this access control scheme is constructed based on the Decentralized -ABE method is introduce by the researcher primer group order (CP-ABE) in reference number [5][8], which is proved to be secure under generic bilinear group model and random oracle model. At an intuitive level, this means that if there are any vulnerabilities in the scheme, then these vulnerabilities must exploit specific mathematical properties of elliptic curve groups or cryptographic hash functions used when instantiating the scheme has emerged as a promising technique to ensure the end-to-end data security in cloud storage system. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. When more and more organizations and enterprises outsource data into the cloud, the policy updating becomes a significant issue as data access policies may be changed dynamically and frequently by data owners. However, this policy updating issue has not been considered in existing attribute-based access control schemes [9] in this paper author are proposed the secure scalable and fine –grained data acecess control for the cloud computing environment .Author Liang –Ao Zhang et.al[10] are proposed the ABE based Access control with the Authentication and proposed the policy for the Cloud . In this paper Researcher are introduce the ABE that is attribute based Encryption technique and used this technique for the providing the securizaion data cloud , In this paper author are focus on the data owner's authentication in the ABE system and proposed a new

scheme for the data access . In this paper author are do the work for Zero Knowledge Proof of Knowledge (ZKPK) to realize the anonymous authentication of the owner's policy updating key without increasing any secret information to the owner side. So authors are propose an access control system with authenticated dynamic policy updating for the cloud storage and our ideas could also be applied to other ABE systems.

IV PROBLEM DESCRIPTION

The policy updating is a difficult issue in attribute-based access control systems, because once the data owner outsourced data into the cloud, it would not keep a copy in local systems. When the data owner wants to change the access policy, it has to transfer the data back to the local site from the cloud, Re-encrypt the data under the new access policy, and then move it back to the cloud server. By doing so, it incurs a high communication overhead and heavy computation burden on data owners. This motivates us to develop a new method to outsource the task of policy updating to cloud server. The grand challenge of outsourcing policy updating to the cloud is to guarantee the following requirements:

i) Correctness: Users who possess sufficient attributes should still be able to decrypt the data encrypted under new access policy by running the original decryption algorithm.

ii) Completeness: The policy updating method should be able to update any type of access policy.

iii) Security: The policy updating should not break the security of the access control system or introduce any new security problems.

V. OVERVIE OF THE EXISTING SYSTEM

Attribute-Based Encryption (ABE) has emerged as a promising technique to ensure the end-to-end data security in cloud storage system. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data. The policy updating problem has been discussed in key policy structure and cipher text-policy structure.

ARCHITECTURAL DIAGRAM

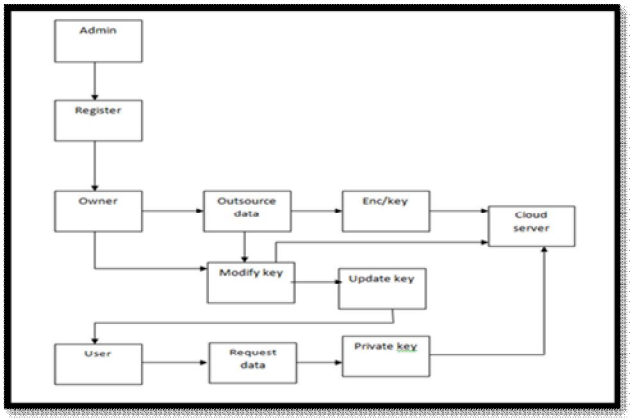

Figure 2: System Architecture

Table 1: Analysis of Data

S.No	Test Condition	Operator Action	Input Specification	Expected Output	Obtained Output
1	Server Login validation	Open login form Enter username as 'server' and no password and click submit button	Enter only user name as input and no password	Alert "Invalid User name and password"	Passed
2	Server Login validation	Open login form Enter username as 'server' and any password and click submit button	Enter only user name as input and any password	Alert "Invalid User name and password"	Passed

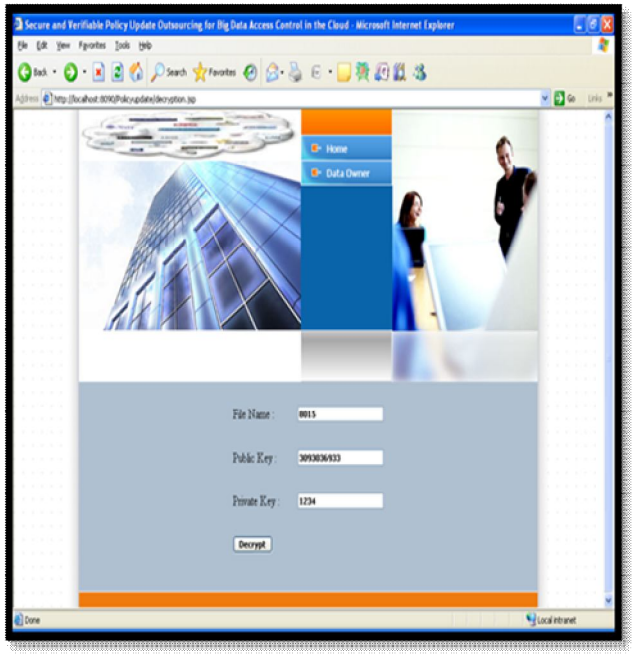

Figure 3: Data Owner File in Big Data

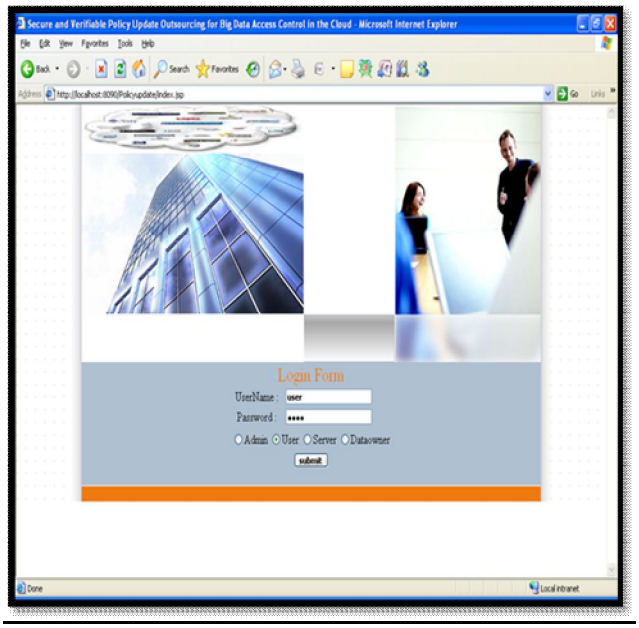

Figure 4: Login Form after polices update Big Data

VI CONCLUSION

It is more efficient for data owners to only generate an update key than generate a cipher text component for each attribute. Attribute-based access control schemes were proposed to ensure the data confidentiality in the cloud. It allows data owners to define an access structure on attributes and encrypt the data under this access structure, such that data owners can define the attributes that the user needs to possess in order to decrypt the cipher text. However, the policy updating becomes a difficult issue when applying ABE methods to construct access control schemes, because once data owner outsource the data into cloud, they won't store in local systems.

REFERENCES

[1]Puya Ghazizadeh, Ravi Mukkamala & Stephan Olariu, 2013,"Data Integrity Evaluation in Cloud Database-as-a-Service", IEEE Ninth World Congress on Services,978-0-7695-5024-4/13, DOI 0.1109/SERVICES.2013.40, pp.280-285.

[2] Ling Lang & Lin wang, 2012, "Research on cloud computing and key technologies", IEEE International Conference on Computer Science and Information Processing (CSIP), 978-1-4673-1411-4/12, pp.863-866

[3] Mohammed A. AlZain & Ben Soh and Eric Pardede, 2013, "A New Approach Using Redundancy Technique to Improve Security in Cloud Computing", pp. 230-235.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS'06. ACM, 2006, pp. 89–98.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in S&P'07. IEEE, 2007, pp. 321–334.

[6] B. Waters, "Key-policy attribute-based encryption(KP-ABE) An expressive, efficient, and provably secure realization," in KC'11. Springer, 2011, pp. 53–70.

[7] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters,"Fully secure functional encryption: Attribute-based Encryption and (hierarchical) inner product encryption(RBAC)" in EUROCRYPT'10. Springer, 2010, pp. 62–91.

[8] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption,"in EUROCRYPT'11. Springer, 2011, pp. 568–588.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM'10.IEEE, 2010, pp. 534–542.

[10] Liang-Ao Zhang et al. " ABE based Access Control with Authenticated Dynamic Policy Updating in Clouds" International Journal of Security and Its Applications Vol.9, No.8 (2015), pp.95-110 http://dx.doi.org/10.14257/ijsia.2015.9.8.08

Taniya Jain has published review research papers in International Journal of Innovative Research in Engineering & Management (IJIREM),ISSN: 2350-0557, Volume-3, Issue-4, July-2016.
Our research work on **"**On Secure Big Data Access Control Policy for Cloud Computing Environment". In other word, I analysis policy updating technique in cloud environment.

