Enhanced Security Framework for Cloud Storage Using Decentralized, Dynamic and Policy-Based Security

Khushbu Malviya[1], Priya Saxena[2]

Research Scholar, CSE, Sanghvi innovative academy, Indore, M.P, India[1]

Lecturer Scholar, CSE, Sanghvi innovative academy, Indore, M.P, India[2]

Abstract: How should the organization can be done to decide what security measures one should have to apply to protect its data and computations, which have different security requirements from a Cloud Service Provider (CSP) with an unspecified or undetermined level of corruption? The answer to this question can be found on the organization's perception about the CSP's reliability and the trustworthiness and the security requirements of its data of an organization. This paper proposes a decentralized, dynamic and evolving policy-based security framework that helps any of an organization to derive such perceptions to provide the proper authority from knowledgeable and trusted employee responsibilities and their functionality are based on that, the choice of the most relevant security policy postulating the confidential measures is very much necessary for outsourcing data and computations to the cloud.

Keywords: Cloud computing, cloud storage, cloud services, Cloud security policy.

I .INTRODUCTION

Cloud computing is a new technology that is a result of wrapping up of virtualization, parallel computing and distributed computing into a single unit. As per the NIST definition of cloud computing we can define it as "Cloud computing is a model for enabling ubiquitous, convenient, on –demand network access to a shared pool of resources (e.g., networks, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". This cloud model is composed of the five essential characteristics, three service models and four deployment models. The term cloud computing is more than a single product; it is very promising and new technology of current time. Cloud computing is consists of two fundamental technique utility computing and service oriented architecture. Cloud computing means to delivery of the complete package i.e. (software, hardware) by internet using any browser. It removes the need and necessity of setting higher cost devices for infrastructure for any of the organization, with the help of cloud computing the organization takes care of its functional work rather than to develop and deploy a costly infrastructure. In cloud environment all the data are outsourced to any external provider and they take care of that data is now a responsibility of the cloud provider and we can access this data on virtual machines or any device. Since the data center of cloud provider is spread to everywhere in the world we can access our data from any corner of the world. It reduces the task of geographical issue.

As we also require the security of our data from the third party to access it, similarly every user on the clouds wanted his data to be secure and confidential. Taken as much consideration of how strongly the provided model is
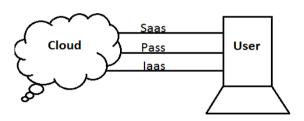

Fig .1 Cloud Computing

secured, consumers continue to suffer from data loss due to lack of trust on the provider. On the other end, the provider faces a complex problem of handling data of such its un-trusted users. Lot of efforts & dimensions has to be wasted while providing such secure architecture & dependency stack. These large numbers of varying dimensions on architecture result in un-managed heterogeneous security controls that must be consistently handled. Security requirements and on applying this requirements the security can be achieved at a bottom level but to increase this level, monitoring should also be implemented to get the better results. the encryption can be done and how the request of the search will be fulfilled. Here by it is very easy to understand the encryption system.

Now with the second example we will discuss the ABE encryption technique. Here, In ABE encryption attributes are defined and it's more briefly discussed as-

Figure.2 represents the encryption technique here, the user here provides his attributes for e.g. his illness which can be fever, diabetes etc., name of the hospital like A,B,C,D, his gender i.e. male or female, his race i.e. Asian, black or white. The user wills provides his all the essential properties and behavior, which are required here.
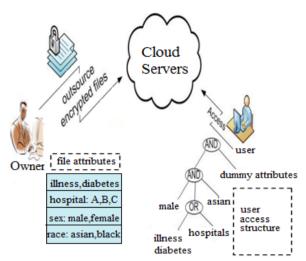
Fig. 2: Attribute based Encryption

Now all the attributes are going to be on the cloud, the cloud is going to merge or focus on all the attributes of the user, these will go to leads to the generation of the key attribute of the user. In this manner the key generation with the help of the attributes is done. In short we can conclude that the key attribute will be generated with the help of all the properties and behavior which will be provided by the data owner. The secret key will be generated with the help of these attributes provided. The secret key is generated to provide the high security which is the base of our motive i.e. our confidential data will be safe and secure. In this figure we also have the user access structure which is represented by the tree with the help of AND a OR properties. The tree has been traversed in bottom up approach to get access to the cloud server.

II.LITERATURE SURVEY

1.A Policy-based Security Framework for Storage and Computation on Enterprise Data in the Cloud Sourya Joyee De, Asim K. Pal,2014 47th Hawaii International Conference on System Science
2.Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds SushmitaRuj, Milos Stojmenovic, Amiya Nayak, IEEE Transactions On Parallel And Distributed Systems Vol:25 No:2 Year 2014.

Previous workings on protected cloud storage and computation have careful consideration on different adversarial models. These models consider a Byzantine adversary, which can be defined as the challenger, which can act as a random, which can corrupt as small number of servers. In this corruption process, the corrupted clouds can blastoff three types of attacks:

1) The storage cheating on corrupted servers can delete rarely accessed files (which means the file which cannot used by user frequently) to moderate the cost of storage or arbitrarily change the stored data.
2) Computation – this is a type of cheating in which the servers either generate improper (incorrect) results of computations or it may uses different inputs for computations going on to reduce computational cost.

3) Privacy- this is a kind of cheating in which corrupted cloud server can leak user's confidential information to other parties. It means that the data of the user is not at all safe the data can be transferred from user's account to other accounts.

Here we can consider that the un-trusted cloud can fail in a Byzantine [4] way i.e. stored user data can be deleted, modified or leaked to other parties and it can result in the argue and argument this causes the most general fault model which results into account both malicious attacks on CSPs as well as events like accidental data corruption. A set of scenarios of different trust levels assigned to cloud has been identified by it. According to them, a trusted cloud is one, which, in the absence of unpredictable failures, serves users correctly in accordance with SLA, and there are no malicious insiders.

III.EXISTING SYSTEM

In Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds **[2],** the owners can only access private files. Highly confidential data must be private and the file policies are set using the confidential features and owner's private attributes. File revocation means making file permanently inaccessible for all including owners and it is done by deleting the secured decryption key with permission of all the owners along with the file policy.

The owners share custom files to a set of selected users. For example, the directors of an organization may share some information to the employees. Among the employees, the owners can select some particular persons also. The persons are authorized with a special access key to access the data, the access permissions like read, edit, download etc are fixed by owners and users don't have any role in that.

All users registered in the system can access public files. A public access policy is set to public files and no specific key needed for users other than their access key to access the public file. Here also the access permissions are set by owners.

IV. PROPOSED SYSTEM

We are proposing the architecture with multiple owners and users. Figure.3 represents the owners of a single data/file may belong to an organization or institution. For example, in a company the confidential data may be handled by only directors and may have more than one director. In such situations the security and integrity of data is challenging.

Here the data may have multiple owners, the owners register into system as a group but having individual access keys and passwords. Anyone in the group can store and share the data. The policies of shared files are set by any of the owners and need approval of all the owners. In short, any change in file policy should need the group permission. The file shared may be private, custom or public based on the set policy.
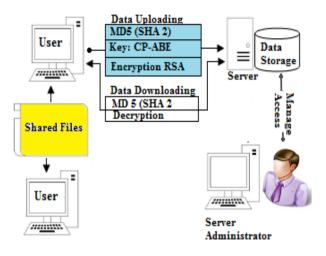
Fig 3: Proposed System Architecture with multiple owner and users.

We perform following operations:
i) Access Key Generation
ii) File Policy and Encryption Key
iii) Decryption
iv) File Revocation
v) Hash Value (SHA2):

Thus the cipher text-policy attribute based encryption scheme consists of four algorithms:

- Setup
- Encrypt
- Key Gen
- Decrypt

KP-ABE may be the dual to CP-ABE within the sense that a good access policy is encoded into the users secret essential, e. g., $(A \wedge C) \vee D$, and a cipher text is computed with respect to a set connected with attributes, e. g., A,B. In this example the person would not be able to decrypt the cipher text but would for instance be able to decrypt a cipher text with respect to A, C.

An important property which should be achieved by both, CP- and KP-ABE is referred to as collusion resistance. This basically shows that it should not be possible for unique users to "pool" his or her secret keys such that they could with each other decrypt a cipher text that neither ones could decrypt independently (which is realized by independently randomizing users' solution keys).

V. CONCLUSION

In this paper we have spoken our ongoing research about a semantic approach about our policy-based security framework for business management processes. We have renowned all the security concerns, which are demanded in day-to-day purpose and these requirements, are classified into two levels that is Task and Process Level. The architecture of security framework is premeditated to maintenance runtime policy controlling and execution. Security policies are built on the top of ontology to enrich representation of security concerns and enable reasoning for the clash of detection and policy negotiations.

REFERENCES

[1] A. Acquisti, and J. Grossklags, "Privacy and Rationality in Individual Decision Making", IEEE Security and Privacy Vol. 3 No. 1, IEEE, 2005, pp. 26-33.
[2] Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds SushmitaRuj, Milos Stojmenovic, AmiyaNayak,IEEE Transactions On Parallel And Distributed Systems Vol:25 No:2 Year 2014
[3] M. A. AlZain, and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44[th]Hawaii International Conference on System Sciences, IEEE, 2011.
[4] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud Computing Security: From Single to Multi- Clouds", 45[th]Hawaii International Conference on System Sciences, IEEE, 2012.
[5] A. Bessani, M. Correia, B. Quaresma, F. Andre, and P. Sousa, "DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds", Proceedings of the 6th conference on computer systems EuroSys'11, ACM, New York USA, 2011, pp. 31-46.
[6] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, ,,Twin Clouds: An Architecture for Secure Cloud Computing", Workshop on Cryptography and Security in Clouds, 2011.
[7] S. Chaves, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing", 6[th]International Conference on Networking and Services, IEEE, 2010.
[8] Y. Chen, and R. Sion, "On Securing Untrusted Clouds with Cryptography", Proceedings of the 9[th]annual ACM Workshop on Privacy in Electronic Society WPES'10, ACM, New York USA, 2010, pp. 109-114.
[9] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, ,, It's All About the Benjamins: An empirical study on incentivizing users to ignore security advice", Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2012, pp. 16-30.
[10] S. De, S. Saha, and A. K. Pal, "Achieving Energy Efficiency and Security in Mobile Cloud Computing", Proceedings of the 3[rd]International Conference on Cloud Computing and Services Sciences CLOSER 2013, SciTePress, 8-10 May 2013, Aachen, Germany.
[11] J. Fontana, "Are human firewalls the enterprise info. sec of the future? http://www.zdnet.com/are-human- firewalls-the-enterprise-info-sec-of-the-future- 7000008497/" (a discussion on Tom Scoltz et al, Gartner's Report on People Centric Information Security Strategy, 2012.)
[12] O.Goldreich,Foundations of Cryptography Volume II Basic Applications". Cambridge, UK: Cambridge University Press, 2004. [12] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", 8[th]IEEE Conference on Dependable, Autonomic and Secure Computing, IEEE, 2009, pp. 711-716.
[13] A. W. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44[th]Hawaii International Conference on System Sciences, 2011, pp. 1-10.
[14] M. Jensen, J. Schwenk, J. Bohli, N. Gruschka, and L. Iacono, "On T echnical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, IEEE, 2009.
[15] M. Jensen, J. Schwenk, J. Bohli, N. Gruschka, and L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds", IEEE 4[th]International Conference on Cloud Computing, IEEE, 2011.