Key Policy- Based Security Framework for Cloud Computing

Ajay Deshmukh [1], Arpit Solanki

*[*1]Research Scholar CSE Department, RKDF SOE Indore, M.P, India.*
[2]Assistant Professor CSE Department, RKDF SOE Indore, M.P, India.

[*1]ajaydeshmukh88@gmail.com, [2]arpit.solanki29@gmail.com

Abstract— A complete acknowledgement about the security concerns is that can the cloud can act as barriers to the adoption of cloud computing which researchers have identified over the last some years. While outsourcing the data on a huge level that means its business-critical data and computations to the cloud, an enterprise loses control over them by the loss of data due to the authority provided on the cloud. 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. The organizational opinion is developed completely direct user participation with that particular organization and is allowed to advance with respect to the time and requirement of an organization.

Keywords— Cloud, Cloud organization, Data privacy, Cloud service provider (CSP), Information Dispersal Algorithms (IDA), Security framework, Cloud security policy.

INTRODUCTION

Cloud computing has given a boom in the present scenario. From each and every enterprise customers are very much reluctant for the deployment of their business on the cloud. But as far as we are concern the security issue is one of the most important and major issue in which gives a negative point and also reduced the vast market of cloud computing and it also result in the complications of the privacy of the data [2]. Data privacy and data protection also get affected from this issue. As we know that in an organization there are several data, which must be kept hidden from the external entities and possesses the sensitivity of the organization's data.

These data can be the very much confidential data like customer data, his private business details, and his family details and so on. Such kind of data would be kept confidential from the third party while exchanging the data [1]. There may be various situations where the data have to flow but they doesn't have permission to change it, for an example employee of the organization needs to access the data of different field respective of his work because of his role in an organization so that would be not to be restricted but any other individual like ordinary employee, supplier and any customer want to access the data then he can only view the data but cannot make any change in it [3]. But with the use of cloud computing we are often in confusion that whether we will outsource the data and its computations on public cloud or not? It includes the loss of control over the data; it will dissolve the concept of the security, trustworthiness of the cloud service provider, data confidentiality, availability of the data and other factors. Some major factors here are legal and Trans border issues, data privacy and data location.

Due to these problems many of the research scholars have tried to resolve this problem and proposed the solution. They have given their contribution in the search of cloud security and their approach has become almost successful also. Their methodology had provided the facility to an organization to outsource their confidential data with security requirements. When an organization is outsourcing its data it is keeping a degree of trust on the service provider of the cloud. The responsibility of the cloud service provider is to protect the data from third party, internal and external attacks [5]. As we know that the agreement between the cloud service provider and organization will be signed which is called service level agreement (SLA).

We had tried to purpose a solution on this problem which is dynamic, decentralized methodology for the highly secure outsourcing on the cloud. Here we can understand the meaning of decentralized as decentralized can be defined as achievement of two taking two accounts, for an example the CEO of the company will tell us the best possible way of the financial sensitive data of his company.

In this paper we will suggest the best possible method of the organizational implementation by our acknowledgement studies.

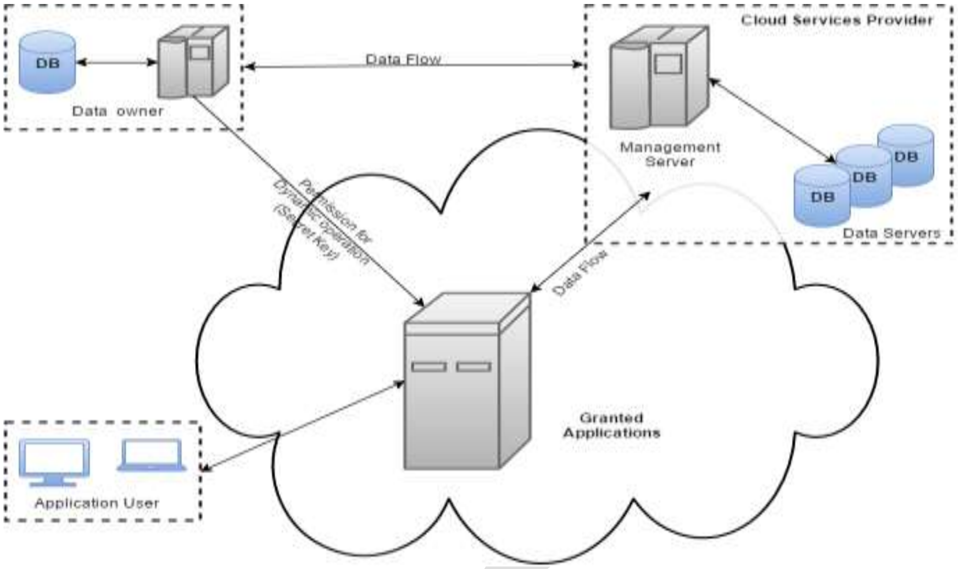

Figure 1.1 Audit System Architecture for cloud computing

The above figure illustrates the cloud computing architecture of the organization. The data owner has its data flow to the data server and management server that is cloud service provider. The application users have to grant the permission to access the data of the organization. First of all the verification will be done and then the permission will be granted to the application user.

LITERATURE SURVEY:

1. A POLICY-BASED SECURITY FRAMEWORK FOR STORAGE AND COMPUTATION ON ENTERPRISE DATA IN THE CLOUD

SouryaJoyee De, Asim K. Pal, 2014 47th Hawaii International Conference on System Science

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 use 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.

Existing System

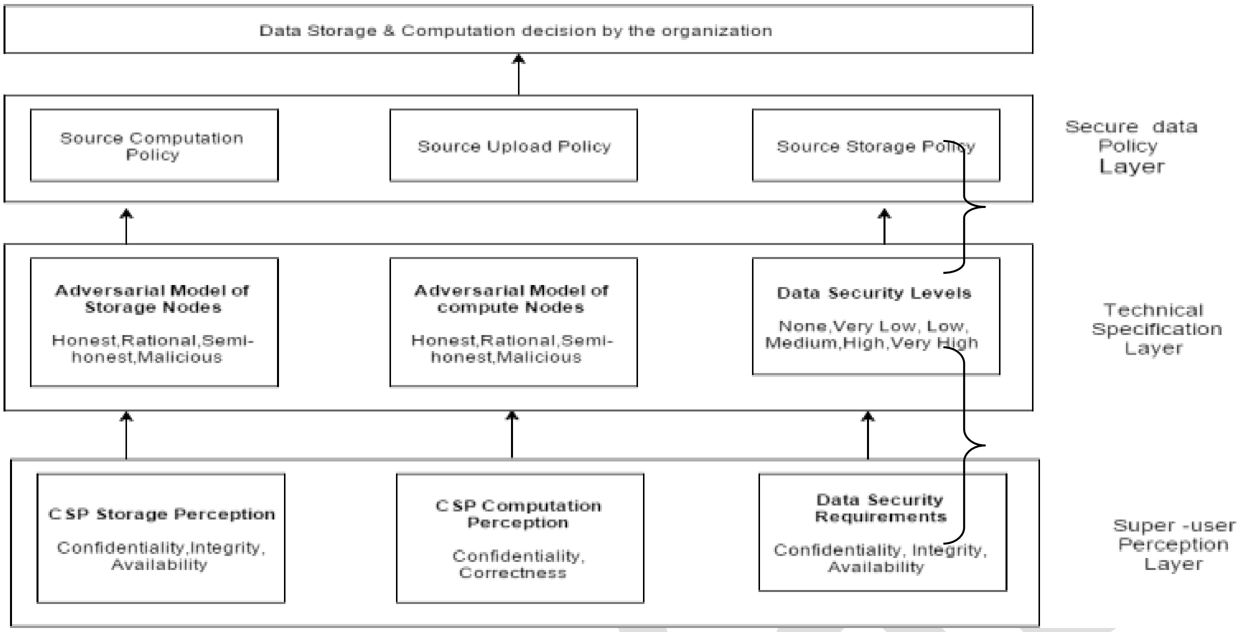
Data Storage & Computation decision by the organization
Source Computation Policy
Source Upload Policy
Source Storage Policy
Secure data Policy Layer
Adversarial Model of Storage Nodes
Honest,Rational,Semi-honest,Malicious
Adversarial Model of compute Nodes
Honest,Rational,Semi-honest,Malicious
Data Security Levels
None,Very Low, Low, Medium,High,Very High
Technical Specification Layer
CSP Storage Perception
Confidentiality,Integrity, Availability
CSP Computation Perception
Confidentiality, Correctness
Data Security Requirements
Confidentiality, Integrity, Availability
Super -user Perception Layer

Figure 1.2 Policy-based Security Framework

There are three basic trust relationships that form the basis of our security framework: organization vs. user; user vs. CSP and organization vs. CSP.[3]

The organization does not trust all the users equally, e.g. people in the top positions are more trusted than others. Users are trusted with only those data and computations that are connected to the role the user is assigned. The organization vis-a-vis user trust relationship is guided by the Enterprise Data Access Policy (EDAP) matrix which tells for each user and data element pair what kind of accesses and rights are permitted. A user who is allowed to choose a security policy for data elements he has access to is called super-user for those data elements.

EDAP Matrix.

Access control matrices specify access rights on objects. An object is the abstraction of resources controlled by a computer system. Role based access control (RBAC)[4] policies regulate a user's access to objects in a system based on the activities he performs on these. We present the EDAP matrix as an intermediate access control matrix derived from role-based access control policies used in the organization. It specifies user's data access rights from which one can validate the computation permitted for each role in the organization. We note that computations require different data elements as inputs and produce new data elements and / or modify existing data elements as output. Therefore, a user can perform a computation only when he has the necessary access rights to relevant input and output data elements [5].

Propose System:

We propose the system with multiple uses and owners. For any organization, Institute confidential file s/data handle by more than one director .in such type of situation data security and authentication is challenging task. We are proposing system have more one owner, each owner having individual access key and password for accessing the data/files of organization. We also define key based policy with following descriptions [3]:

- Data store and share in-group by any owner.
- Policies created by any owner but need approval by all owners
- Changing in policy, all owners' permission needed.
- Owner can only access private files.
- Registered users can access public files which uploaded by owner.

- Public file access policy is defined by all owners.

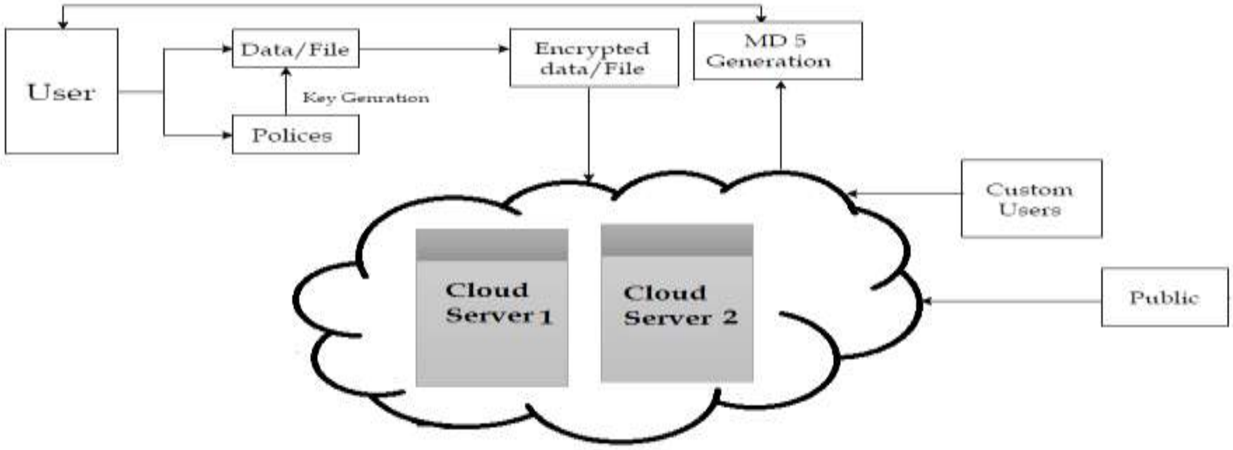

Figure 1.3 Proposed System

Proposed system consists of following Operation:

- **Key Generation:** Access secret is generated for every user UN agency registers within the system. System collects some attributes from user as well as identity attributes like e-mail, user-name etc. mistreatment these attributes and a few alternative options a singular secret is generated and from that key, employing a pattern operate, a 6 digits code is passed and generated to the user [7]. In propose system three type of users
  - Owner
  - Public User
  - Customer

- **Define Access Policy and Encryption Key**: File Access policies are generated for every file supported the confidentiality of the file. The owners might store the file as non-public, public or custom and should set the permissions as scan, edit, transfer and delete.

- **Decryption:** Before accessing a file, the file policies and user policies are matching. If each matches, then per the access key of user the system finds the permissions allowed for that user and retrieves the mix code. The key codes are retrieved and combined to form the key. Then secret writing is doing thereupon key.

- **File Revocation:** File revocation suggests that creating the file for good inaccessible. Deleting the file policies and coding keys will this. Deleted the key can't be reformed and secret writing is not possible. Once a file is making an attempt to access, initial the file policies are checked, if there's no file policy then there itself the file is inaccessible. The system twice ensures the inconvenience of a file [9].

- **Hash Value (MD-5):** Generate the hash price for store file on cloud. MD5 processes a variable-length message into a fixed-length output of 128 bits. Those functions are as follows:

$$F(A,B,C) = (A \wedge B) \mid (\sim(A) \ \& \ C)$$
$$G(A,B,C) = (A\& \ B) \mid (B \ \& \sim(C))$$
$$H(A,,B,C) = A \wedge B \wedge B$$
$$I(A,B,C) = A \wedge (B \mid \sim(B)$$

Proposed Algorithm:

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., $(A\wedge C)^{V}$ 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).

Algorithms of for KP-ABE with enhancement are discussed as below:

KP-ABE Key Generation (A, M_K):

Proposed algorithm output a secret key D added with a access structure T. Following three step describe access structure A:

1. Every root node represent with r, set secret value = y.

2. Using loop each non leaf node

   a. If the ^ (And) operator and all child node mark with unsigned.

   b. If the ^{V} (OR)operator), and Mark this node as assigned and set value s.

3. For each leaf attribute a_j,i ε T , compute D_j;i = T_j∧si

   Secret Key S_k= { D_j,i}

4) KP-ABE Decryption (E, D): Proposed algorithm takes input as cipher text (E) using the attribute policy decrypted the Message with secret S_k and public key Pk.

ACKNOWLEDGMENT

I especially thank to Mr. Arpit Solanki for stimulating and helpful discussion on IDS and helping me to clarify my ideas

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] 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] M. A. AlZain, and E. Pardede, “Using Multi Shares for Ensuring Privacy in Database-as-a-Service”, 44th Hawaii International Conference on System Sciences, IEEE, 2011.

[3] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, “Cloud Computing Security: From Single to Multi- Clouds”, 45th Hawaii International Conference on System Sciences, IEEE, 2012.

[4] 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.

[5] 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.

[6] S. Chaves, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing", 6th International Conference on Networking and Services, IEEE, 2010.

[7] Y. Chen, and R. Sion, "On Securing Untrusted Clouds with Cryptography", Proceedings of the 9th annual ACM Workshop on Privacy in Electronic Society WPES'10, ACM, New York USA, 2010, pp. 109-114.

[8] 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.

[9] S. De, S. Saha, and A. K. Pal, "Achieving Energy Efficiency and Security in Mobile Cloud Computing", Proceedings of the 3rd International Conference on Cloud Computing and Services Sciences CLOSER 2013, SciTePress, 8-10 May 2013, Aachen, Germany.

[10] 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.)

[11] 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", 8th 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", 44th 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, "On T echnical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, IEEE, 2009.