International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 10 5762 - 5766

Policies and User Perception based Data Security in the Cloud

Ms. Rakhi Ramdas Dighade (PG Student)
Department of Information Technology
Sinhgad College of Engineering,
VadgaonBudruk, Pune, India
rakhi.dighade@gmail.com

Mrs. S. M. Jaybhaye (Assistant Professor)
Department of Information Technology
Sinhgad College of Engineering,
VadgaonBudruk, Pune, India
smjaybhaye.scoe@sinhgad.edu

***Abstract*—**In today's world, most of the companies migrated from desktop devices to the cloud. Cloud is a platform for storing large amount of data. Among this it is very necessary to provide data security over the un-trusted cloud. We cannot trust the cloud provider when sensitive data is stored in the cloud so that, various security aspects are required to protect sensitive data which is stored on the cloud. The main problem is that, how to deal with such security issues to protect sensitive data. With the help of policy based security, it is possible to minimize data security issues and to improve data privacy. This paper proposes a user perception framework. According to this framework, owner of the organization is able to tell which user of that organization will follow which rights. A particular user should provide his/her privileges to the owner and he will protect user's data by giving full rights to access data based on the identification of the users.

Keywords*-Access rights; Cloud computing; cloud security; perception; policies.*

*****

I. INTRODUCTION

With this emerging technology of cloud computing in the environment, employees of the organization still hesitate to outsource their data in the cloud. Security is a major concern in cloud computing. The organization wants to store all the sensitive data over the cloud which proves to be confidential, maintains integrity and ensures availability [2]. The organization does not include only employees but also includes other members of the enterprise. Therefore, it is a prime concern of whether to outsource the data and computations to the cloud or not. This, in turn has hyped to implement security policies for data outsourcing and computation that are either too lax or too strict, making it either insecure or inefficient, respectively. It may be performing too many costly activities (such as encryption, decryption, huge data upload/download during computations etc) that may offset the benefit of using the cloud in the first place. Similarly, it may be performing too few security activities putting its data at risk [3].

Clouds consist of multiple network-connected resource clusters such as server farms, data warehouses, and so on that host geographically distributed virtual machines and storage components that ensure scalability, reliability, and high availability. A multicloud system that employs proxies for collaboration consists of three architectural components: multiple cloud computing systems, networks of proxies, and clients (or service users). Such systems can use several possible strategies for placing proxies in the proxy network. In the current situation the users of the enterprise data e.g. grocery chain and vendors require to develop their understanding of the sensitivity and criticality of the applications and data they handle also their perceptions about trustworthiness of the CSP based on their own interactions with the cloud while performing their job on the cloud. Two studies reported that user participation contributes to improved security control performances through better awareness and alignment between Information System Security Risk Management (ISSRM) and the business environment and improved control development [3]. There is hardly any holistic approach that can help an organization to take decisions about which data or computation to outsource based on sensitivity or security requirements. And how to do so securely based on its perception about data sensitivity and the trustworthiness of the CSP. When data and computations are outsourced to the cloud, the organization bestow a certain degree of trust on the CSP to take proper security measures to protect its data and applications from external as well as from insider attacks. In response to "privacy crisis", systems and tools have been developed to offer strong privacy protection for users' cloud data, such as information flow control, secure and trusted operating systems, secure hypervisors, and novel anonymization and encryption schemes. Despite their high degree of technical sophistication, these tools have yet to empower users with control over their cloud data [4, 5].

II. LITERATURE SURVEY

A. Policy Sealed Data

Nuno Santos et al. [6] had proposed PCD abstraction inspired by Excalibur, which offers policy-sealed data, another abstraction for building trusted cloud services. Like PCD,

Excalibur uses CP-ABE to encrypt customer data and bind it to a customer-chosen policy. Excalibur imposes a high barrier on the cloud-service infrastructure. In contrast, the goal with PCD is just to ensure that the cloud provider explicitly opts-into the customer policy–no heavy-weight enforcement mechanisms are necessary. Its advantage is that it reduces the overhead of key management and improves the performance of the distributed protocols employed.

B. Policy and context management

Canh Ngo et al. [7] had suggested an on-demand provisioned access control infrastructure with dynamic trust establishment for entities in a Cloud IaaS architecture model. It uses authorization ticket as a security session management mechanism to solve the security context synchronization and exchange between multiple Cloud providers. The author had described practical implementation of the proposed Dynamic Access Control Infrastructure as the part of a complex infrastructure services provisioning system.

C. Attribute based encryption in scalable and secure sharing

B.Vamsee et al. [8] had proposed a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. The author has used ABE technique to encrypt the data. The author has suggested secure data outsourcing mainly in multiple data owners. This scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. A PHR owner can update her sharing policy for an existing PHR document by updating the attributes (or access policy) in the ciphertext. The author has allowed add/modify/delete option to the user.

D. Privacy preserving authorization system

David W et al. [9] had described a policy based authorization infrastructure that a cloud provider can run as an infrastructure service for its users. It protects the privacy of users by not allowing the unauthorized users. The users are allowed to set their own policies as required. This infrastructure also ensures the enforcement of privacy policies which may be written in different policy languages by multiple authorities such as: legal, data subject, data issuer and data controller.

III. IMPLEMENTATION WORK

In order to retain control over the data and computation resources on the cloud a policy based security is designed. Policy based security converts user perceptions into computations. The set of policies are elaborated called as the secure data policies consisting of storage security policies, upload security policies and computation security policies to guide the organization in finding out the right security level for each combination of data security requirement of the CSP. It develops a people centric highly evolving and dynamic organizational view of the outsourcing operation of the enterprise data via the cloud. Figure 1 shows the block diagram of policy based security. We have discussed the block diagram such as how the user at the individual level as well as the enterprise at the organization level express their data security requirements and CSP trustworthiness based on which we arrived at the security policies.

1. Users are the trusted employees of an organization who are required to register first and this registration is done by the admin.
2. Admin is be the system who will do the registrations of the users of the organization.
3. Cloud service provider who manages the cloud servers, request the data to the cloud data storage and stores the data in the cloud.
4. Cloud data storage stores the data of the users in the cloud.
5. Cloud is the entity that gives the requested data to the admin after verifying the user's policies.

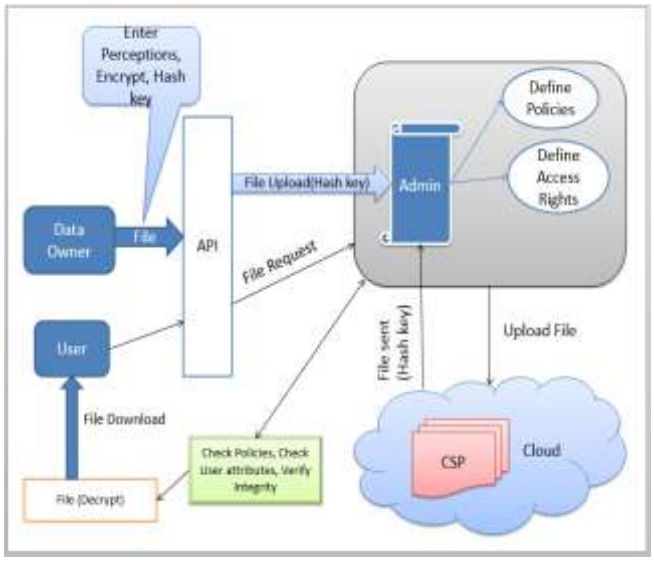

Figure 1. Cloud security based architecture using policies

A. Attributes as perceptions

Admin converts the perceptions into policies. The perceptions are given as attributes when uploading file. The file is given as input to the system. The admin then asked to enter the perceptions for the file security. Security is given in terms of confidentiality, integrity and availability. User achieves confidentiality by encrypting the file. Integrity is achieved by generating hash code.

For more security, along with the perceptions the file is encrypted using ABE. User apply perception that the file

should only be viewed to Amdocs company. So while uploading file the data owner apply the perception as "Company Name: Amdocs". Policies can be in the format:

Company name: Amdocs or Microsoft for the Position: Manager with Experience 12 to 20 at Location Pune

So this file is visible to only people who are from company Amdocs Or Microsoft for the position of Manager with 12 to 20 years of experience located at Pune.

The EDAP matrix is enterprise Data Access Policies matrix. This matrix contains policy related information about data access from the cloud. It tells which rights should give to which users to access data from the cloud. This helps in increasing data security and data privacy when data is stored on the cloud.

IV. RESULTS AND DISCUSSION

This paper is implemented in java using MYSQL database. This paper is implemented using NetBeans. NetBeans is free integrated development environment use to run java source code. It provides full support from development life cycle to the debugging of the code. The IDE runs on Windows, Linux, Mac OS X, and other UNIX-based systems. For cloud deployment, cloud server is used. At first new instance is created and then project deployed on that instance. Following are some results:

A. Upload File

When user uploads file, he has to apply perceptions over the file for file security. The user will enter one by one field to enter the perceptions. The user will upload the file in the encrypted format and hash key will also be generated. Figure 2, shows the user perceptions to upload file.

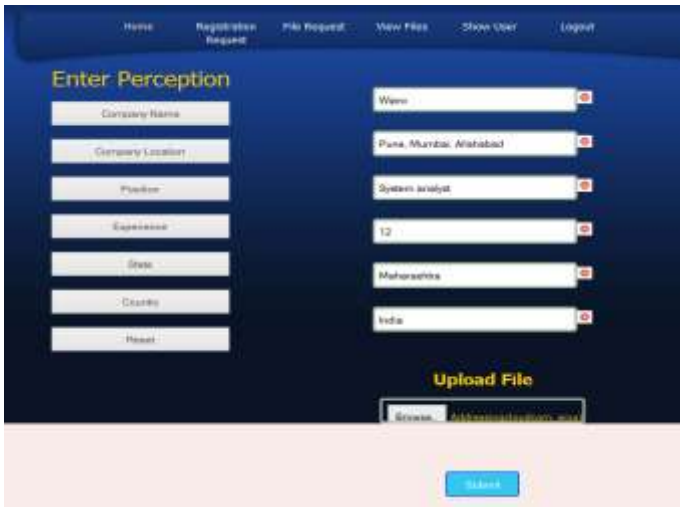

Figure 2. User perceptions to upload file

B. File Policy

When the user uploads the file, he enters the perceptions. That perceptions will get converted into the file policy. When he uploads the file encryption is done and hash key will be generated and saved in the database of the admin. If the user updates the file then regenerated hash code entry will be filled up.

Figure 3. View policy

C. Send user attributes to the admin

The user will click on the checkbox to verify the user. These attributes will be generated when user registers into the system. These user attributes are then sent successfully to the admin. The file request is now sent to the admin.

Figure 4. Send attributes to the admin to request file

D. Secret Key

When other user wants to download the file, a file request is sent to the admin. If admin approves the file request then at the user's side, a key is to be entered by the user which is sent by mail on his registered email id. User policies are shown in figure 5.

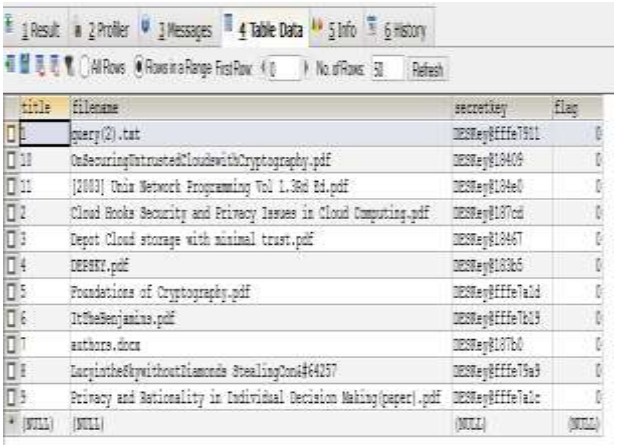

Figure 5. User policies

 ISSN: 2321-8169
5762 - 5766

E. Attribute verification

In attribute verification, as shown in figure 6. the admin will verify the user and the file according to the policies applied by the data owner while he uploads file. If the file policy matches with the user attributes then admin will approve the user and email id is sent at the registered email id of the user.

Figure 6. Attribute verification for file and user

F. Upload the file with encryption:

According to the file size, time is required to upload the file as shown in figure 7.The user has uploaded the file with file id 1 its time required to upload is 0.09500 ms. The last file with file id 11 required the time 3.34400 ms.

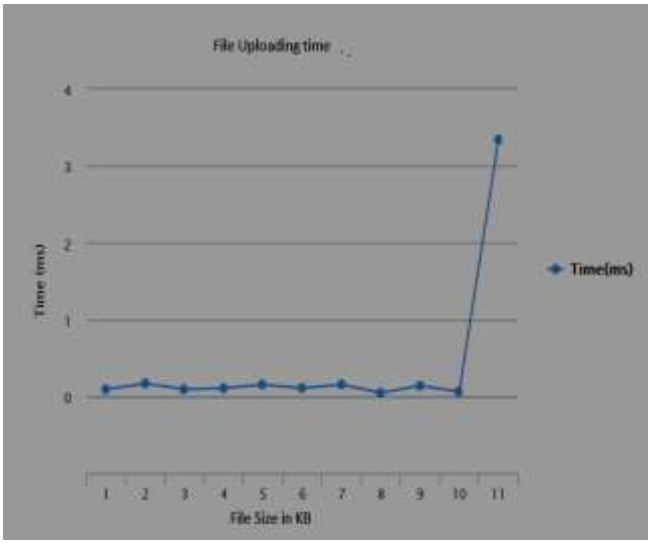

Figure 7. File encryption in uploading

G. Download the file with decryption:

Figure 8. shows the file decryption time that is computed when the user downloads the file. For the file with file id 1 required 0.0001 ms to download. For the file with file id 7 required 0.00123 ms to download.

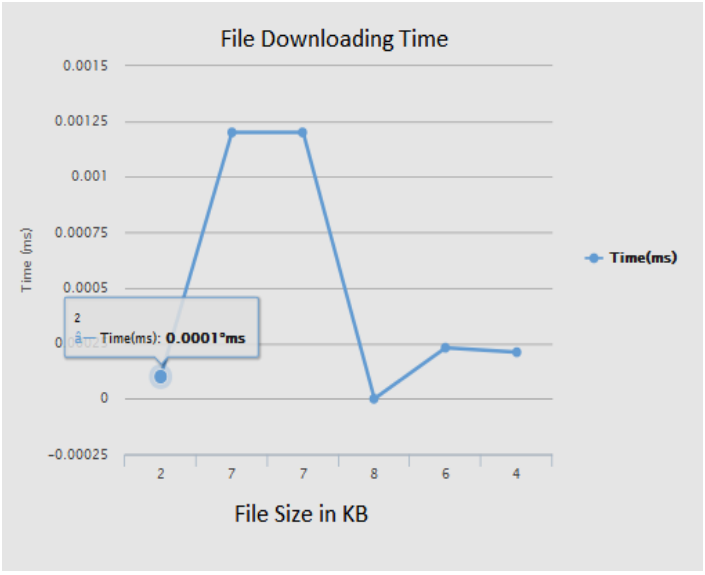

Figure 8. File decryption in downloading

H. Comparison of existing AES and implemented AES:

The comparison graph is shown in figure 9, is generated for existing AES and AES with ABE. The time required for implemented AES for file id 2 is 0.078 ms.

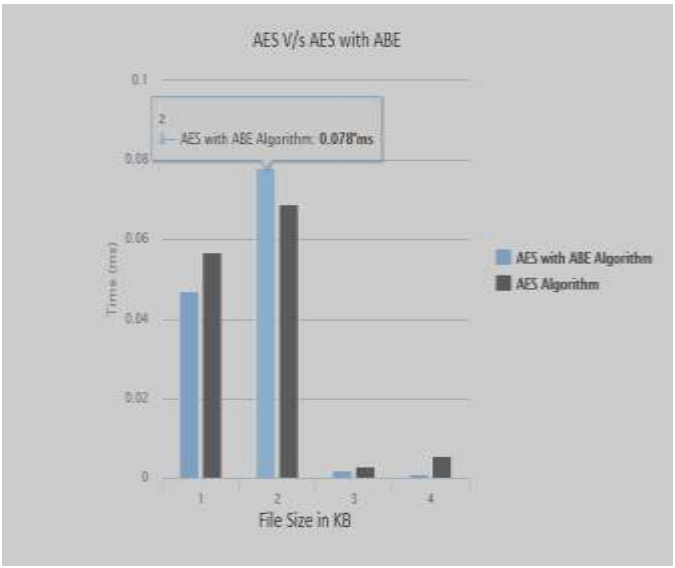

Figure 9. Comparison of AES and AES with ABE

V. CONCLUSION AND FUTURE SCOPE

This paper proposes a policy based framework with the concept of user perceptions. This helps in securing outsourced data by any attackers or unauthorized parties. Policies are attached to data according to user perception. One EDAP matrix is there which helps employees which data to be get accessed by knowing policies in EDAP matrix. This will increase the degree of security to the cloud data.

ACKNOWLEDGMENT

I would like to express my gratitude towards Mrs. S. M Jaybhaye for their persistence guidance throughout the project.

I would like to thank Mrs. B. P. Vasagi for their constructive criticism and Mrs. Sonar for their valuable support.

REFERENCES

[1] SouryaJoyee De, Asim K. Pal, "A Policy-based Security Framework for Storage and Computation on Enterprise Data in the Cloud", 2014 47th Hawaii International Conference on SystemScience,978-1-4799-2504-9/14, 2014 IEEE DOI10.1109/HICSS.2014.613.

[2] G. Greendwald and E. MacAskill, "Boundless Informant: the NSA's secret tool to track global surveillance data." The Guardian – http: //www.theguardian.com/world/2013/jun/08/ nsa-boundless-informant-global-datamining, 2013.

[3] P. Gill, V. Erramilli, A. Chaintreau, B. Krishnamurthy, K. Papagiannaki, and P. Rodriguez. "Follow the money: Understanding economics of online aggregation and advertising". In IMC, 2013.

[4] S. Zdancewic, L. Zheng, N. Nystrom, and A. C. Myers, "Untrusted Hosts and Confidentiality: Secure Program Partitioning", In ACM SOSP, 2001

[5] S.Chong, J. Liu, and A. C. Myers. "Sif: Enforcing Confidentiality and Integrity in Web Applications", In USENIX Security Conference, 2007.

[6] N. Santos, R. Rodrigues, K. Gummadi, and S. Saroiu. "Policy-Sealed Data: A New Abstraction for Building Trusted Cloud Services". In USENIX Security Conference, 2012.

[7] C Ngo, P Membrey, Y Demchen, University of Amsterdam1, Hong Kong Polytechnic University2 email: {t.c.ngo, y.demchenko, delaat}@uva.nl1, peter@membrey.hk2, Reliability and Security, "Policy and Context Management in Dynamically Provisioned Access Control Service for Virtualised Cloud Infrastructures", 2012 - ieeexplore.ieee.org

[8] B. Vamsee Mohan, M. Rajani , Pbr Vits, Kavali, Nellore, Andhra Pradesh, India, "Attribute-Based Encryption of Scalable and Secure Sharing in Personal Health Records using Cloud Computing", Volume 4, Issue 7, July 2014, ISSN: 2277 128X

[9] David W Chadwick and Kaniz Fatema, University of Kent, Canterbury, CT2 7NF, "A Privacy Preserving Authorisation System for the Cloud", Journal of Computer and System Sciences, 2012 – Elsevier