Securing Enterprise Data using Policies and User Perceptions in the Cloud

Rakhi R. Dighade
PG Student: Dept. of Information Technology
Sinhgad College of Engineering
Pune, India
Email: rakhi.dighade@gmail.com

Mrs. S. M. Jaybhaye
Assistant Professor: Dept. of Information Technology
Sinhgad College of Engineering
Pune, India
Email: smjaybhaye.scoe@sinhgad.edu

***Abstract*— Security agitations are an important factor that behaves as a hurdle in the adoption of cloud environment. Data outsourcing is an emerging factor in cloud computing. In this the client shares his data with the owner which in turn sends the data to the cloud service provider (CSP). The clients have to outsource the critical data related to business to the cloud. Therefore organizations have to protect the content of the data while outsourcing as it loses the control over the data. But the major problem arises as to how to secure the business related data. So Policy based security is proposed which provides security to the user's data and protect against other human threats. This work is based on user's perceptions which tell the owner of the organization which rights should be given to which user. The genuine user can provide the privileges to the owner of an organization. The owner will protect the data of the genuine user by giving him the full rights of his data based on the perceptions of the users**

Keywords- Cloud computing, policy, user perceptions, cloud security, access rights

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 [2]. According to Gartner, user participation plays a very crucial role in security. Two studies with information technology governance, audit and security, found out that security can be improved involving users participation with greater awareness and improved alignment between security management and governance [13]. It helps to secure the data which involves control of users. Awareness also can be developed between management groups and business entrepreneurs [3].

Organization bestows certain degree of trust over the cloud users when it outsourced their data and computations. Therefore, securing the outsourced data and having control over the data has peacocked the enterprise. Also, SLA is also between the cloud users and CSP"s. Monitoring requires keeping track on these agreements. Such monitoring can be done by cloud providers, business groups or a third party. Therefore, organizations must build their own perception about how the CSP will behave i.e. to what extent it can be trusted with different items of data and computations. This will help building policies to retain control over data and computations outsourced to the cloud. A trust based system is developed that involves direct user participation, their perceptions are taken as input and providing them the access rights. Gartner suggested that when users are given the responsibility to handle the data then security can be ensured. A policy based security is beneficial and flexible minimizing the risk of data corruption. The super user handles the encryption of data, uploading of data, defining polices and giving the access [1].

II. RELATED WORK

In Depsky system [4], Depsky protocol CA is used that uses secret sharing and erasure code techniques. Fig. 1, shows the Depsky model with four clouds. This technique is used for replication of the data in cloud of clouds. In this system, using the encryption key the original data block is encrypted. The key shares along with the shares of the data are erasure coded. The fig below shows four erasure coded blocks as four clouds are given. If anyone provider is untrusted then there is possibility of loss and change of data.

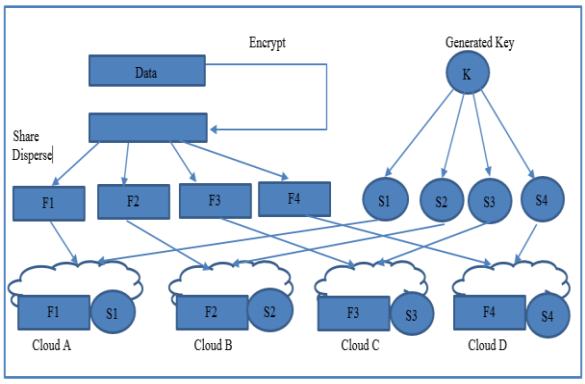


Figure 1. Depsky model with four clouds

Secure multiparty computation [5] compares real-world execution of a protocol for computing an n-party function *f* to the ideal-world evaluation of *f* by a trusted party. In MPC, dishonest players are modeled by a single adversary that is allowed to corrupt a subset of the parties. Dishonest workers can choose not to participate in the computation, can compute on arbitrary inputs, or abort the computation prematurely. The cloud provider is assumed to be semi-honest in secure multiparty computation.

The general data service outsourcing architecture involving three entities [6]. Fig. 2, shows the privacy search using trapdoors. The data owner (or data contributor) is one or multiple entities that generate, encrypt data and upload them to the cloud server. The cloud server within a cloud service provider CSP) possesses significant storage and computation resources and provides them to the end users in a pay-per-user

manner. There are one or more data users in the system, which may need to perform queries over the outsourced data in order to extract useful information. To enable search access by the users, the data owner usually generates and distributes cryptographic keys or "trapdoors" to the users, either actively or upon user's requests. When a user wants to initiate a query, he/she submits a corresponding trapdoor to the server, who carries out the search and returns the results in an encrypted format. In some situations, the data user and data owner can be the same physical entity. The disadvantage is that it does not guarantee service availability in case of failures.

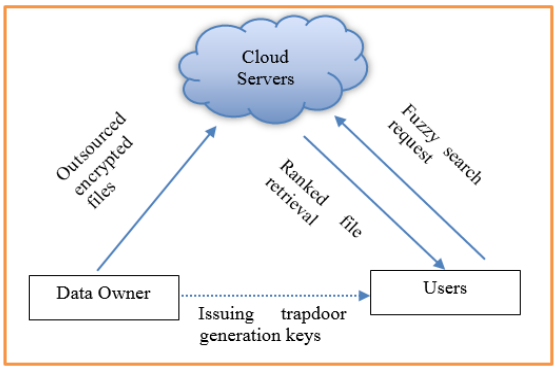


Figure 2. Privacy search using trapdoors

In CloudSeal the content is encrypted at cloud database. Only authorized end users or the content provider can decrypt it. It applies dual encryption algorithm on plaintext then uploaded to the cloud. Here proxy is used that sends the ciphertext to the delivery network. In order to decrypt the provider updates the proxy re-encryption keys. CloudSeal splits the ciphertext of the content stored in the cloud into two parts, so that the proxy only re-encrypts a very small part of ciphertext, and the large portion remains unchanged. Only authorized users can obtain the latest decryption key, and the content provider maintains the control of issuing new keys. K-out of-n secret sharing renews the shared secret key in a scalable fashion [7].

In general policy enforcement framework [8] author have considered three modules viz. data type, computation and policy requirements. In policy requirements they stated the access control policies, data sharing policies, privacy policies, etc. The author have also proposed policy-compliant data processing framework were these four modules are considered 1) Policy-reasoning module where the policies are applied on the data which performs specific tasks 2) Data processing task rewriting module Pre-processing module Post-processing module. The author have used XACML policy based security mechanism which checks that the user can access the underlying table or views. Although the use of XACML makes difficult to update the decision criteria after governing policy changes.

In a unified system, Flexible authorization manager (FAM) [9] obsolete multiple access control policies. FAM is responsible for accessing the objects by giving authorizations and access control policies. It is usually based on a language that holds all security specifications. Users can specify their own protection policies for the information they own from the authorization library. The author have stated three policies viz. closed policy, open policy and hybrid policy. The flaw in this system is that a user is allowed to choose only one type from the three policies as a clash can happen if number of types are specified for different objects.

The author suggested classical and mandatory policies [10] and using the intersection of these policies. Although using these two polices do not solve the practical requirements. Role based access control provides better security than mandatory policies.

The author have used encryption policy [11] using selected encryption technology. This technique uses different keys for encrypting data and gives to each user a set of keys that allow her to decrypt all and only the resources she is authorized to access. Although the use of such encryption policy does not assist the CSPs because of large community and also there bakes a change in information.

In current CDSA [12], a Trust Policy (TP) module implements policies defined by authorities or institutes. The main drawback of a TP in current CDSA is that trust policies are hard-coded by its developer. It would be more flexible if users were able to define and modify deployed trust policies for their application domains. It has been observed that the problem can be fixed by adding a policy interpreter to CDSA.

III. PROPOSED WORK

In order to retain control over the data and computation resources on the cloud a policy based security is designed as shown in figure 3. 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 and perceived adversarial behavior of storage and computation nodes (VMs) 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. We discuss the building blocks 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.

- Users are the trusted employees of an organization to whom the admin gives the access rights according to the data elements he uploads.
- Super user is higher authority who uploads the data of the user to the cloud in the encyrpted format.
- Cloud service provider who manages the cloud servers, request the data to the cloud data storage and stores the data in the cloud.
- Cloud data storage stores the data of the users in the cloud.
- Cloud is the entity that gives the requested data to the admin.

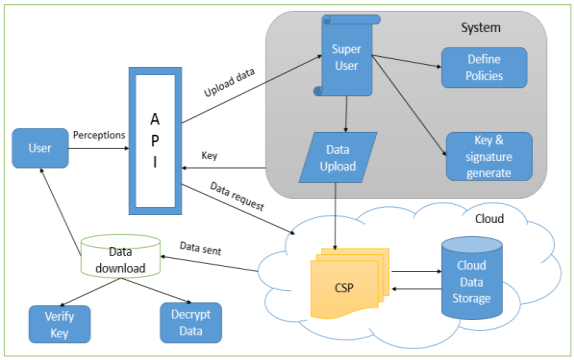


Figure 3. Policy framework for secure storage.

A. *User perceptions*

Gartner suggested that when users are given the responsibility to handle the data then security can be ensured. Even though SLA is there to sign the agreement with the CSP still providers have to update the latest SLA. Users will have to think that the data they have provider will be required this level of security, the CSP can be vulnerable or not and to what extent it can harm their data. Unless you are not responsible for particular work, you cannot measure the right security level. This process is efficient and dynamically will achieve the perfect security to user's data. Users can give their perceptions on the basis of previous experience such as any security breach incidents, security certifications, etc. User perceptions are given in terms of confidentiality, integrity and availability to the organization admin. Employees of the organization have to give proper training about how they can bestow the right level of perception regarding the vulnerability of the cloud service providers. Lack of education and being unknown with the CIA cycle of security will again constraint to protecting data. Therefore, a cloud service provider should be chosen such that it could rarely have security breaches.

B. *User interface*

It will be used to receive the user's requests, data storage, data upload and user perceptions and also displays outputs of computations to the user.

C. *EDAP matrix*

Enterprise Data Access Policy matrix tells the organization which access rights are allowed to which user. All the roles of single user, their access rights and the policies are maintained in the matrix. This matrix is derived from the EDAP filter which checks the unauthorized access to the particular data element. If the user has performed the write access for which he is not authorized then after three attempts he will be debarred from the login for that particular day. And if that user wants to have the read access then a notification will be sent to the super user about change of access and after checking again the roles and policies and previous attempts he has performed access rights can be changed. For more security, session can be maintained for the user login. A certain time period only is given to the browsing of data or uploading the data. The EDAP matrix having the user access rights is shown in table 1.

Table 1. EDAP matrix

Elements	User 1	User 2	Policies	
			User 1	User 2
Data 1	Read	Write	Data 1 read computation should be performed at single VM	Data 1 write computation should be performed at single VM
Data 2	Write	Read	Data 2 write computation should be performed at the single VM	Data 2 read computation should be performed at the single VM

a) *Role Based Access Control (RBAC)*

It is used to regulate the access on data objects the user performs. Higher responsibility of users are assigned as the super user roles.

b) *Define Policies*

Policies are the set of rules that guide the organization to identify each and every user in the enterprise. Secure computation policies are given for computation. Different policies should be there for different users. For example, in the university the policies such as, the person with ten years of experience with the knowledge of cloud will only be allowed to access the files related to cloud. Not all the users who are having the right to access the customer details are allowed to also access the credit card details. The following table 2. Shows the user registration form.

Table 2. User registration form

UID	User 1	User 2
Name	A	B
Email id	a.R@gmail.com	b.R@yahoo.com
Age	21	23
Access	Read	Write
Password	******	******
Technology	Cloud	Data mining
Position	IT analysts	Project Manager
Place	Pune	Pune

1) *Secure computation policy*

- A single VM performs computations.
- Semi-honest for other than 'None' and 'Medium' security data, a single VM is given a random number of challenge computations before the actual computation.
- Computations on other data are done by a single VM.
- A single VM can perform computations on public data.
- A single VM can perform computations for security level 'None'. For Low and Very Low security data, a single VM is given the Challenge.

2) *Secure storage and upload policy*

- All data stored in plaintext by the user

- Uploaded plaintext should be encrypted.
- Public data with very low sensitivity should be stored in plaintext at the user side while every public data should be uploaded in encrypted format.

D. *Control box*

The policy based security is handled using Control box. In fig 6. Policy controller diagram is shown. It contains an EDAP filter which is used to filter all the access rights of the authorized and unauthorized user, user perceptions and three controllers. If the user has tried to access the 'write' even though he is not allowed to access then a control box will object the user and move the user to the first place of the login side. A control box has three components:

a) Policy controller

It receives super user perceptions about data and gather the data requirements

b) Data and storage controller

It will be helpful to generate shares of data (if considered), digitally sign the data and upload the data to selected storage node. It will also retrieves the data when the user requests the data, will check the integrity.

c) Computation controller

Selected computation will be performed by the users upon requests.

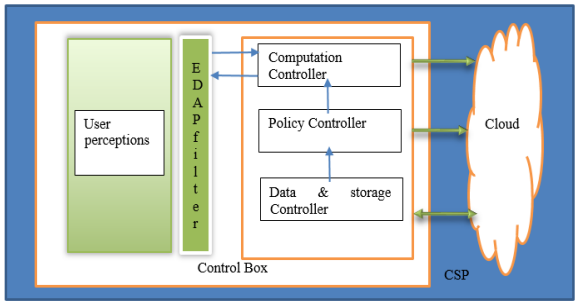


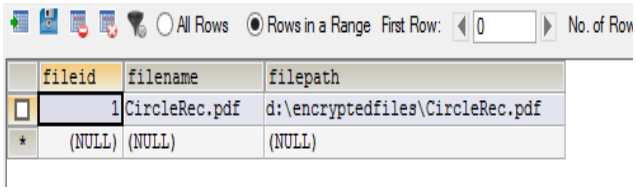
Figure 4. Policy Controller

E. *NetBeans IDE*

NetBeans IDE is a free, open source, integrated development environment (IDE) that enables you to develop desktop, mobile and web applications. The IDE supports application development in various languages, including Java, HTML5, PHP and C++. The IDE provides integrated support for the complete development cycle, from project creation through debugging, profiling and deployment. The IDE runs on Windows, Linux, Mac OS X, and other UNIX-based systems. MySql database is used to store the user profile. Amazon EC2 is used for storage compute. At first an instance is created whenever a new user wants to have the storage. The instance is created from the Amazon management console.

IV. RESULTS

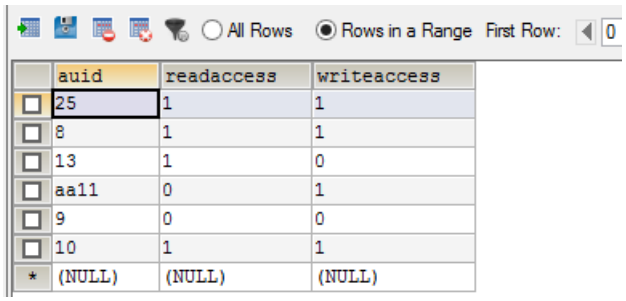
A user has to register first to upload their data. After registration user can login into the system whenever he wants. After the successful registration user sends the data to the super user. Super user then define the policies, encrypt the data and then uploads it to the cloud. Figure 5. Shows the encrypted file and filepath.



fileid	filename	filepath
1	CircleRec.pdf	d:\encryptedfiles\CircleRec.pdf
(NULL)	(NULL)	(NULL)

Figure 5. Encrypted file and filepath

Each user is given the user ID at the time of registration. Super user given the read and write access to the user and fig shows the database of the super user. If read and write access is given to the user then input is '1' otherwise '0' is input. Figure 6. Shows access alloacation to user.



auid	readaccess	writeaccess
25	1	1
8	1	1
13	1	0
aa11	0	1
9	0	0
10	1	1
(NULL)	(NULL)	(NULL)

Figure 6. Access allocation to user by the superuser

Secure upload policy stores the user's data for a particular. Each user will be given the user ID and correspondingly will apply the policies. Figure 7. Shows the policy allocation to the user by the super user.

Secure upload policy	Requirement
All data stored in plaintext	Yes
Uploaded data should be encrypted	Yes
Low sensitivity data stored in plaintext	None

Figure 7. Policy allocation to the user by the superuser

V. CONCLUSION AND FUTURE SCOPE

This system will provide more security to the uploaded data in the CSP due to the appliance of policies on the user's data based on user's perceptions and roles in the organization. EDAP matrix will be helpful to guide the organization and its employees. A filter will check the unauthorized access. All the data will be uploaded in the encrypted format and only one key will be used for encryption and decryption.

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. R. S. Sonar for their valuable support.

REFERENCES

[1] Sourya Joyee 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 System Science, 978-1-4799-2504-9/14, 2014 IEEE DOI 10.1109/HICSS.2014.613

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", J. Network and Computer Applications, 34 (2011) 1–11.

[3] J. L. Spears and H. Barki, "User participation in information systems security risk management", MIS Quarterly, Vol 34, Issue 3, 2010, pp. 503-522I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[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, 2011Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[6] M. Li, S. Yu, K. Ren, W. Lou, and Y.T. Hou, "Toward privacy-assured and searchable cloud data storage services," IEEE Networks, vol. 27, issue 4, pp. 55-62, July/August 2013.

[7] H. Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen, "Towards End-to-end Secure Content Storage and Delivery with Public Cloud", Proceedings of the 2nd ACM Conference on Data Security and Privacy CODASPY'12, ACM, New York USA, 2012, pp. 257-266.D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467

[8] S Jajodia, P Samarati, VS Subrahmanian, "A Unified Framework for Enforcing Multiple Access Control Policies", ACM Sigmod Record,1997,dl.acm.org

[9] RS Sandhu, P Samarati, "Access control: Principle and practice, Communications Magazine, 0163-6804/94/$04.00@IEEE, 1994 - ieeexplore.ieee.org

[10] KW Hamlen, L Kagal, M Kantarcioglu, "Policy Enforcement Framework for Cloud Data Management", IEEE Data Eng. Bull., 2012,utdallas.edu

[11] S De Capitani di Vimercati, S Foresti, S Jajodia, "Preserving Confidentiality of Security Policies in Data Outsourcing", Proceedings of the 7th, 2008, dl.acm.org

[12] A Lin, R Brown, "The Application of Security Policy to Role-Based Access Control and the Common Data Security Architecture", Computer Communications, 2000-Elsevier

[13] A Loske, T Widjaja, A Benlian, P Buxmann - 2014 - aisel.aisnet.org "Percieved IT security risks in cloud adoption: The role of perceptual incongruence between users and providers", Twenty Second European Conference on Information Systems, Tel Aviv 2014