ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Secure Data Sharing in Cloud for Distributed Accountability using Patchy Image Encryption

Swapnil Dattatraya Taru[1]
Computer Engineering (Computer Networks)
K. J. College of Engineering & Management Research
Pune – India

Prof. Vikas B. Maral[2]
Computer Engineering (Computer Networks)
K. J. College of Engineering & Management Research
Pune – India

Abstract: ***The global widespread use of Cloud computing has enabled highly scalable services that could be easily provided to consumer created new challenges by introducing different types of trusts scenario. Cloud computing promises to increase the flexibility with which applications are deployed at lower costs while increasing business agility.***

The important feature of cloud services is that user's data are usually processed remotely and users do not own these remote machines or operate them in cloud. Users can lose control of their own confidential data though some privacy protection techniques concentrate on some preventive controls, research is needed for better controls in the area of accountability and protecting privacy.

Despite of all of advantages of cloud this remains a challenge and acts as a barrier to the large scale adoption of cloud. To address above problem in this paper we present a novel highly decentralized information accountability framework called as CIA (Cloud Information Accountability) that will protect user's data and also monitor the data flow in cloud. We propose the object oriented approach that performs automated logging mechanism to ensure any access to user's data will trigger authentication.

We use the object oriented JAR (JAVA Archive File) programmable capabilities to create dynamic travelling object containing user's data. To strengthen the distributed data security we use the chaos image encryption technique specific to image files. Chaos is patchy image encryption technique based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data.

Keywords: Cloud computing, accountability, data sharing, logging mechanism, chaos encryption.

I. INTRODUCTION

Cloud Computing is incessant growing latest technology in the business, IT sector and academia. Cloud computing is highly scalable, flexible technology that puts hardware, software, and virtualized resources.etc ie.computing infrastructure over the internet on demand basis. Main feature of cloud computing is that scalability, storage and processing data remotely and provides shared services to user on demand basis in distributed environment. Nowadays there are number of individuals and commercial cloud computing service providers are present including Google,Yahoo,Microsoft,Amazon etc.[12].The details of cloud services are abstracted from users. Moreover, users are unaware of location where machines which actually process and host their data. This also imposes threat because while enjoying the flexibility brought by this new technology, users also start concerning about losing control of their own data.

The data processed on clouds are can be outsourced, leading to a number of issues related to accountability and privacy such as handling of personally identifiable information. Hence these can become disadvantages in maintaining privacy and protection to their data to sustain confidence in potential customers. Data owner use different services provided by cloud service provider also shares data among different cloud users as shown in fig 1.

Accountability and privacy issues regarding cloud are becoming a significant barrier to the wide adoption of cloud services. There is a lot of advancement takes place in the system with respect to the internet as a major concern in its implementation in a well effective manner respectively. Many of the users are getting attracted to this particular technology due to the services involved in it followed by the reduced computation followed by the cost and also the reliable data transmission takes place in the system in a well effective manner respectively.

To overcome these problems approach used is Cloud Information Accountability (CIA) framework based on Information Accountability (IA) [1]. The proposed CIA framework can provide accountability and secured data transferring through novel use of image encryption technique in a distributed manner. This comes with usage control, access control, and authentication. By means of CIA, data owners can track whether the service level agreements agreed and enforce access and usage control rules.

Fig.1 Cloud Storage

The design of CIA framework presents certain issues, that includes unique identification of cloud service provider (CSP), keeping log away from tempering, Decentralized infrastructure etc.We use and extend the programmable capability of JAR (Java Archives) files to automatically log the usage of the users' data. Users will send their data in encrypted form. In our case we use chaos image encryption to encrypt images that are enclosed within JAR files along with access control policies and upload them on cloud service providers.

Any access to the data will trigger an automated logging mechanism local to the JARs. Such decentralized logging mechanism helps to keep the dynamic nature of the cloud but also imposes challenges on ensuring the integrity of the logging [1].The rest of the paper is organized as follows: Section 2 discusses related work. Section 3 proposed system and section 4 concludes the paper.

Currently we concentrate on image files as images represents a very common content type for users on social networks and organizations [7].Images are increasingly on the cloud as a part of storage service which is provided by different cloud service provider (CSP).Moreover images are often content type for sharing on social networks or for archiving important files in organizations.

In addition, our approach can handle personal identifiable information provided they are stored as image files (they contain an image of any textual content, for example, the SSN (Security Social Number) stored as a .jpg file. We use the chaos image encryption algorithm for image encryption. Chaos is suitable for image encryption, as it is closely related to some dynamics of its own characteristics [6]. The behavior of the chaos system, under certain conditions, presents phenomena which are characterized by sensitivities to initial conditions and system parameters.

II. Related Work

A. Security and Privacy Issues:

A. Title: "Accountability as a Way Forward for Privacy Protection in the Cloud"

Author: S. Pearson, A. Charles worth, "Proc First Int'l conf. Cloud Computing, 2009".

Summary: Pearson et al. have proposed accountability mechanisms to solve privacy issues of end users.They proposed method in which cloud service provider defines certain policies respective with owner's stored data.This approach has limitation that data is not stored in unencrypted form so there is threat of data leakage.Authers developed new method called as privacy manager [4].In this Pearson Suggested that user's private data can be put on cloud in an encrypted form and then processing is done on this data at CSP.

A privacy manager mechanism was given by S. Pearson in which the user's data is in encrypted form in cloud and evaluation is done on encrypted data. The privacy manager makes readable data from result of evaluation manager to get the correct result. As in obfuscation data is not present on Service provider's machine so there is no risk with data and hence data is safe on cloud. But this solution is not suitable when input data is large where this method can still require a large amount of memory.

B. Title: "Ensuring Distributed Accountability for Data Sharing in the Cloud".

Author: Smitha Sundareswaran, Dan Lin, "IEEE Transaction on dependable a secure computing, 2012"

Summary: In this paper, the authors propose a novel automatic logging mechanism in the cloud. To our knowledge, this is the first suggested approach for data accountability through the novel use of JAR files. They proposed CIA architecture in which data owner uploads data with access policies enclosed within jar file [1]. This jar is uploaded on cloud service provider. Their suggested architecture is platform independent and also highly distributed. In this approach there is no need of purposeful authentication or storage. But the main drawback of this method is it stores multiple inner jars, which takes a lot of time to execute there is possibility of tampering JAR files also encryption is not used.

C. Title: "The Design and Evaluation of Accountable Grid Computing System".

Author: W. Lee, A. Cinzia Squicciarini, and E. Bertino, "Proc.IEEE Int'l Conf. Distributed Computing Systems"

Summary: In this paper they proposed another approach. A distributed approach assuring the accountability in grid based computing system. Accountability is an important aspect of any computer system. Because every action executed in the system can be traced back to some entity. It also assures the safety and security in grid systems, given the very large number of users active in these sophisticated environments. Their work addresses such insufficiency by developing a comprehensive accountability system driven by policies and supported by accountability agents.

In this paper they first discuss the requirements that have driven the design of their accountability system and then present some interesting aspects related to their accountability framework. They describe a fully working implementation of their accountability system, and conduct extensive experimental evaluations. Their experiments, carried out using the Emulab testbed, demonstrate that the implemented system is efficient and it scales for grid systems of large number of resources and users. But this approach is mainly focused on resource consumption and tracking of sub jobs processed at multiple nodes the notion of accountability policies are based on user also single point failure causes the whole system unusable.

D. Title: "Provable Data Possession at Untrusted Stores".

Author: R.Curtmola, J.Herring, L.Kissner, Z.Peterson, "Proc. ACM Conf. Computer and Comm. Security"

Summay: In this paper they suggested method for security of data in cloud. In their work they used a Provable Data Possession (PDP) model that allows a client to verify that the server possesses the original data. It supports large data sets in widely

distributed storage system. It provides better efficiency, does not have any restriction on the format of the data. But this model has grater block access complexity Proposed model allows to check integrity of the data stored on cloud without retrieving at client side [2]. This model suggests the probabilistic proof of possession by sampling random sets of blocks. PDP scheme does not include any error correcting code.

B. Image Encryption Techniques:

A. Title: "A New Hybrid-Domain Image Encryption based on Chaos with Discrete Cosine Transform"

Author: R. Krishnamoorthi, P.Murali, "International Conference on Electronics Computer Technology"

Summary: Authors proposed a new hybrid-domain image encryption technique. It uses the frequency-domain encryption with Discrete Cosine Transform (DCT) with multi resolution approach and spatial domain for pixel shuffling. First, original image divided into significant and insignificant blocks using prewitt's edge detector operator and significant blocks are encrypted using Arnold cat map and Logistic map. Next, insignificant blocks are shuffled in the DCT domain using Arnold cat map then inverse DCT applied and pixels in the blocks are XORed with discretised output of logistic map. Finally, diffusion process is applied to get final encrypted image and the numerical simulations have demonstrated the security and robustness of the proposed encryption scheme [9].

B. Title: "Logistic chaotic maps for binary numbers generations"

Author: Ali Kanso, Nejib Smaoui, "Chaos, Solutions and Fractals"

Summary: In this paper author suggested method of encryption. The first stage comprises of encrypting the image using Henon map and the second stage confuses this encrypted image using logistic map. The first stage comprises of three steps [11]. The first step represents the plain image matrix into a row matrix and generates an image dependent array. The second step generates a chaotic sequence using Henon map with initial values dependent on above array. The third step encrypts the image as a function of this chaotic sequence. This algorithm encrypts the image successfully but during decryption of the image the entire image is not recovered.

III. OBJECTIVES

We take the CIA (Cloud Information Accountability) framework as a base for our paper. And we propose the extended CIA framework to satisfy following objectives:

- Data must be only used by end user who has the authorization to access the data provided by the data owner and not by the CSP.
- Log files should be regularly sent back to data owners to inform current usage of their data to detect misuse.
- Log files should be kept tamper proof and data should be kept leakage proof.
- In any case of misuse of data the corresponding data owner can have access details of an end user.
- Providing Auditing Facilities based on Log records.
- As a further extension use improved image encryption for data protection and authorization.
- More generalized access to owner's data in distributed environment.

IV. System Design

The Cloud Information Accountability framework proposed in this paper conducts automated logging with enhanced image encryption and distributed auditing of data access performed by end user, carried out at any point of time at any cloud service provider(CSP).It has two major components: logger and log harmonizer.

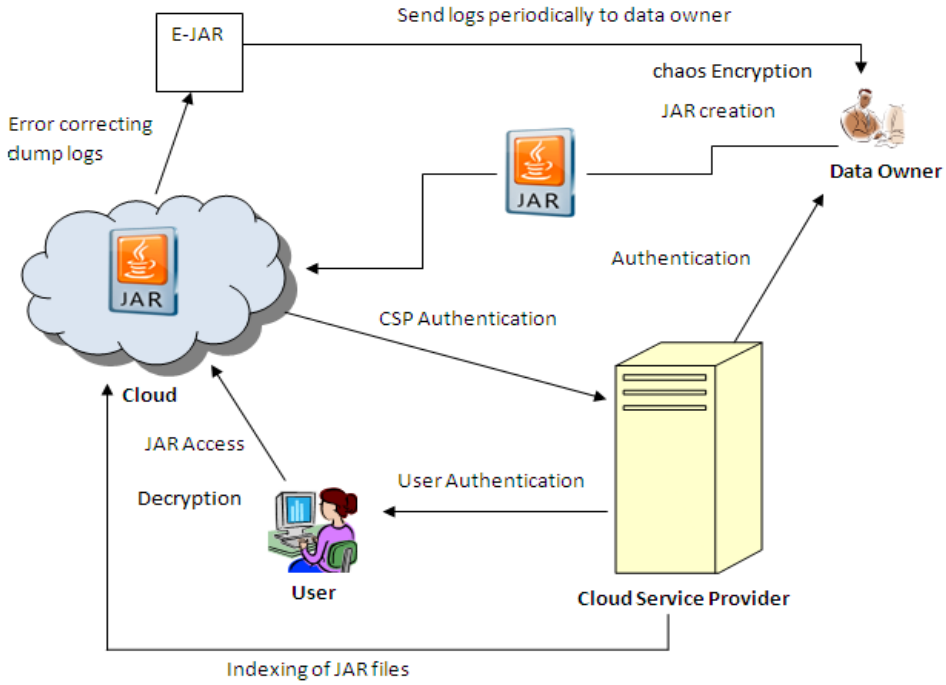

Fig.2 System Architecture

1. Logger component:

Data owner will create the logger component in JAR file to store the data items. The JAR file contains outer JAR and Inner JAR. The major accountability of JAR is to hold the authentication of entities and it requires accessing the data that are stored in the JAR file. Every Inner JAR consists of encrypted data and class files to recover the log file, the log file for every encrypted item.

2. Log harmonizer:

The encryption of the log file avoids the unauthorized change to the file by attackers. The log harmonizer is to hold the log file corruption and the logger send the error correction information in to the log harmonizer.

3. Log record generation:

In CIA framework logs are created by logger module. Logger module will create logs at any access to the data present in JAR file. Newly created logs are appended sequentially in order to produce log record (LR).Each Log record contains information of end user in tuple format as follows:

LR = < Username, Location, File name, Action, Date and time >.

4. Chaos Encryption:

As our proposed work mainly focuses on image type files we use the enhanced Chaos image encryption algorithm for encryption of image file in Jar file. Chaos is patchy image encryption technique based on pixel scrambling where in the randomness of the chaos is made utilized to scramble the position of the data.

The proposed method utilizes the randomness of the chaos maps in order to encrypt the image. In this algorithm the pixel are shuffled according to the randomness of chaotic element attributes, which can be derived by comparing sorted and unsorted elements using Henon map.

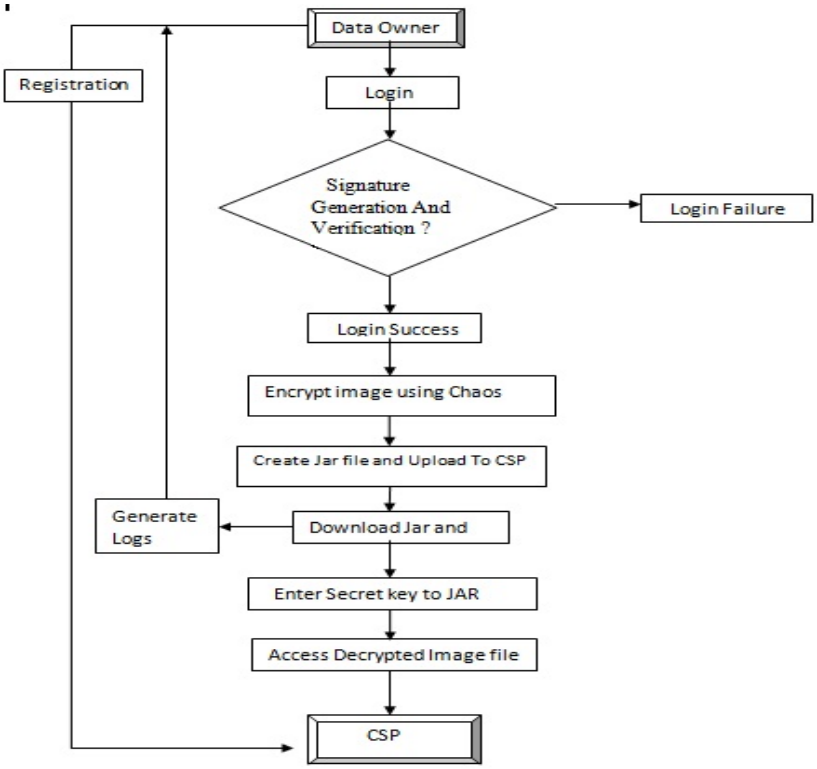

Fig.3 Data Flow

The overall CIA framework is shown in Fig.2. At the beginning, the data owner will login will username and password. Then data owner will encrypt image file and create a JAR file which act as the logger component, to store its data items. Then data owner uploads the JAR containing the encrypted image file to the cloud service provider (CSP).End user authenticated by CSP who want access to data can download jar containing encrypted data. End user can send request to data owner for secrete key to access data. After proving keys by data owner user can open jar file and can have access decrypted image file.

V. CONCLUSION

In this paper we propose an Innovative approach for automatically logging scheme and image encryption technique that provides security to data in the cloud along with an auditing mechanism. We can use Object oriented approach to protect the data using Jar file and enhanced chaotic image encryption method. It is more important to protect people's privacy on the cloud, against unwanted and unauthorized access of their confidential data. We can improve the efficiency of CIA framework by using encrypted logged files, chaos image encryption technique and use of jar file. This paper presents effective mechanism, which performs automatic authentication of users and create log records of each data access by the user. Data owner should not worry about his data on cloud using this mechanism and data usage is transparent.

References

1. Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin,"Ensuring Distributed Accountability for Data Sharing in the Cloud,", IEEE Transaction on dependable a secure computing, VOL. 9, NO. 4, pg 556-568, 2012.
2. S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Proc. First Int'l Conf. Cloud Computing, 2009.
3. W. Lee, A. Cinzia Squicciarini, and E. Bertino, "The Design and Evaluation of Accountable Grid Computing System", Proc.IEEE Int'l Conf. Distributed Computing Systems (ICDCS '09).
4. S. Pearson, Y. Shen, and M. Mowbray," A privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (cloudcom), pp.90-106,2009.
5. B. Chun and A. C. Bavier,"Decentralized Trust Management and Accountability in Federated System," Proc. Ann. Hawaii Int'l Conf. System Science (HICSS), 2004.
6. Chen Wei-bin; Zhang Xin; "Image encryption algorithm based on Henon chaotic system" Image Analysis and Signal Processing, 2009. IASP 2009. International Conference, Publication Year: 2009 , Page(s): 94 – 97.
7. Flickr, http://www.flickr.com, 2012.
8. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598- 609, 2007.

9. R. Krishnamoorthi, P.Murali," A New Hybrid-Domain Image Encryption based on Chaos with Discrete Cosine Transform", 4thInternational Conference on Electronics Computer Technology, IEEE 2012.

10. S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, “Promoting Distributed Accountability in the Cloud,” Proc. IEEE Int’l Conf. Cloud Computing, 2011.

11. Ali Kanso, Nejib Smaoui. Logistic chaotic maps for binary numbers generations. Chaos, Solitons and Fractals,vol.40, pp.2557-2568,2009.

12. P.T. Jaeger, J. Lin, and J.M. Grimes, “Cloud Computing and Information Policy: Computing in a Policy Cloud?,” J. Information Technology and Politics, vol. 5, no. 3, pp. 269-283, 2009.

