An Efficient Approach using AES for Accountability in Cloud

Rintumol Joseph
Department Of Computer Science and Engineering
PG Scholar.
Amal Jyothi College Of Engineering
Kottayam, Kerala,India

Fabeela Ali Rawther
Department Of Computer Science and Engineering
Amal Jyothi College Of Engineering
Kottayam, Kerala,India

Merlin Mary James
Department Of Computer Science and Engineering
Mangalam College Of Engineering
Kottayam, Kerala,India

ABSTRACT
Cloud computing promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing business agility. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. This lead to a situation that the owner may have a fear of loss of data. To avoid this problem the term accountability has been introduced here. Here the owner's data information are stored in the jar file. At the uploading time, one time password concept has been used to give more security to the data.log file access by the owner by either push or pull algorithm is also made much secure with an AES approach. Here we have proposed a novel algorithm for Log push and pull method which is comparatively simple than the existing approaches.In that AES has been is applied. We provide implementation details that describe the efficiency and effectiveness of the proposed approaches.

General Terms
Cloud computing, logging, One time password, AES.

Keywords
Accountability,jar file concept,Log pull and log push method.

1. INTRODUCTION
Numerous surveys report that Cloud Computing will be a top 10 technology that enterprise business managers need to be aware of. Cloud Computing is a lower cost delivery model for IT services. Cloud computing promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing business agility. Cloud computing that allows it to support every facet, including the server, storage, network, and virtualization technology that drives cloud computing environments to the software that runs in virtual appliances that can be used to assemble applications in minimal time[1].

Cloud computing amplifies computer security issues that have proliferated with the growth of the Internet. A broad range of security research is being applied to cloud computing. This paper gives a description of cloud computing followed by a general description of information security issues and solutions, and a brief description of issues linking cloud computing with information security. Security solutions must make a trade-off between the amount of security and its performance cost and impact on the end-user experiences. This is accentuated in a cloud computing environment where users desiring different levels of security share the same resources. An essential issue for cloud computing is the perception of security, which is beyond the simple technical details of security solutions. This paper includes a list of a few key information security challenges that also present significant research opportunities. Solving these key problems will encourage the widespread adoption of cloud computing. build, and deliver applications, and the architectural considerations that enterprises must make when adopting and using cloud computing technology.

Cloud Information Accountability (CIA) framework[2][7], based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, information accountability focuses on keeping the data usage transparent and trackable. Our proposed CIA framework provides end-toned accountability in a highly distributed fashion. One of the main innovative features of the CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed. Here we also take a new approach with AES algorithm for security because it is highly efficient, not so complex, and very secure. One Time Passwords are better way of using user name-password based authentication. We use one time password concept to make sure the accountability concepts in the cloud are more secure.

2. CLOUD COMPUTING –A NEW ERA INFRASTRUCTURE.
The term „cloud computing" is made up of two terms, cloud and computing. Cloud could be thought to be synonymous with the Internet where various resources are interlinked with the use of network. One can use the resource they want with the help of simple client-server architecture. The term computing" refers to processing. Cloud computing is computing on various resources over the network.

Service models
The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) as shown in figure 1. In a Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system,

hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

Characteristics

The characteristics of cloud computing include on-demand self service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centres. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

Deployment of cloud services:

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud[8].

Generally speaking, services provided by a **public cloud** are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.In a **private cloud**, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party. In a **community cloud**, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider.

A **hybrid cloud** is a combination of different methods of resource pooling (for example, combining public and community clouds)[1].

2. Accountability concepts in cloud

It is a mechanism in which user's data is safe on cloud , in this technique the user's data is in encrypted form in cloud and evaluating is done on encrypted data, the privacy manager make readable data from result of evaluation manager to get the correct result. In obfuscation data is not present on Service provider's machine so there is no risk with data, so data is safe on cloud, But this solution is not suitable for all cloud application, when input data is large this method can still require a large amount of memory.

Accountability is also the checking of authorization policies and it is important for transparent data access. We provide automatic logging mechanisms using JAR programming which improves security and privacy of data in cloud. Using this mechanism data owner may know his/her data is handled as per his requirement or service level agreement.Accountability is defined as "the obligation and/ or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations", accountability goes beyond responsibility by Obligating an organization to be answerable for its actions.The trust towards use of resources is accomplished through accountability so to resolve problem for trust management in federated system they have given three layers architecture, in first layer is authentication and authorization in this authentication does using public key cryptography. Second layer is accountability which perform monitoring and logging. The third layer is anomaly detection which detects misuse of resources. This mechanism requires third party services to observe network resources.Cloud information accountability framework is introduced in order to proceed the automated logging and distributed Auditing mechanism which consists of two component namely logger and log harmonizer[2].

3. RELATED WORK

3.1 LOGGING MECHANISMS

The Cloud Information Accountability framework proposed in this work conducts automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time at any cloud service provider.It has two major components: logger and log harmonizer.

Logger component: Data owner will create the logger component in JAR file along with 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. It offers Pure Log and Access Log. The PureLog, records only the general information about every access. Access Log, Records general information and also the time duration. It supports four types of actions, i.e., perform has one of the following four values: view, download, timed access, and Location-based access.

A. PureLog. Its main task is to record every access to the data. The log files are used for pure auditing purpose.

B. AccessLog. It has two functions: logging actions and enforcing access control. In case an access request is denied, the JAR will record the time when the request is made. If the access request is granted, the JAR will additionally record the access information along with the duration for which the access is allowed.

To carry out these functions, the inner JAR contains a class file for writing the log records, another class file which corresponds with the log harmonizer, the encrypted data, a third class file for displaying or downloading the data (based on whether to have a PureLog, or an AccessLog)We are using AES technique to keep the log files as protected. The outer JAR may contain one or more inner JARs, in addition to a class file for authenticating the servers or the users.

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. To guarantee trustworthiness of the logs, every record is signed by the entity accessing the content. After that the entity records should be hashed together and to generate the chain structure, so it can easily detect the errors and missing records. To verify the integrity, the encrypted log files can be converted in to the decrypted form. Every log harmonizer is in charge of copies of the logger components contains the similar set of data items.

Log record generation: Log records are generated by the logger component. Logging occurs at any access to the data in the JAR, and new log entries are appended sequentially, in order of creation LR = <r1; . . . ; rk>. Each record ri is encrypted individually and appended to the log file. In particular, a log record takes the following form: ri =<Username,Loc,File Name,Act,Date,Year,T> Here, ri indicates that an entity identified by ID has performed an action Act on the owner's data at time T at location Loc.

4. ARCHITECTURE OF OUR NOVEL APPROACH

The overall architecture combining owners, data in jar file,cloud service provider,user,logfile generation,users as shown in Figure 3.At the beginning,Owner can sign up and then corresponding jar file will be created .Then the owner can login and upload the data to that jar file.

The dataowner will get a one time password with which he/she is authenticated to upload the data.The uploaded files will be stored in the corresponding jar file.On the net,user will be provided with a sign up and then sign in through which the user can access the data.On each action performed on the data ,it will be recorded and keep in a log file which is encrypted by AES algorithm.A secret key will be given to the data owner with which he can decrypt the log file and get the log records.

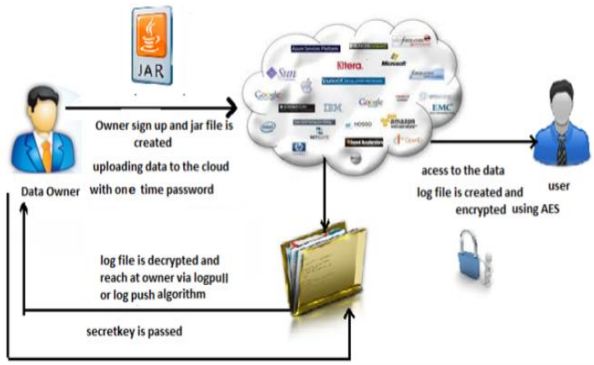

Figure1. New Architecture

5. ONE TIME PASSWORD SCHEMES

are used by almost all business applications for authentication. However static passwords have lots of limitations e.g. passwords can get hacked; careless employee may write down passwords somewhere; system with saved passwords may be used by various users or a malicious user may reset all passwords just to create havoc. Hence it is advisable to move to a more dynamic password scheme like one time passwords or OTP.OTP generation can be done by various OTP generation algorithms for generating strings of passwords.In our approach we provide a one time pass word for the uploading purpose where we can have give some more accountability. The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources, like a computer account. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced.The proposed system attempts to alleviate the problem of shoulder surfing or eves dropping by making the replay of a password useless. Every time a user is authenticated by totally different password[4].At the time of uploading the owner will get a one time password in his mobile and then he has to enter it to do further actions.

6. ADVANCED ENCRYPTION STANDARDS SCHEME IN CLOUD

This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths; however they are not adopted in this standard. Throughout the remainder of this standard, the algorithm specified herein will be referred to as "the AES algorithm." The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavours" may be referred to as "AES-128", "AES-192".

The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length.Here a new approach such that where we go for AES to give security for the log files which contains log records[5].When a user access a data own by an owner,a log record id generated and kept in the log file which will be in an encrypted format.When the owner follow a log pull method to get his log file,he should enter the secret key by which that log file will be decrypted and accesable by that owner.

7. LOG PUSH AND PULL ALGORITHM

1.Pull=0,;

2.rec=<Uname,ip,Location,Filename,AcessType,Date, Year,Time>

3.lsize=size of log file

4.list=list in log file

5.if (lsize<size and pull !=0)// If an action performed

Log file=rec+ENCRYPT();//Log file is created and Encrypted using AES.

6. If(Key==original Key)//Log pull

Log file=log file+DECRYPT()'//Log file is decrypted using the key

//Logs will be displayed.

7.Set Time period as tp//log push

8.if(time=time+tp)

Emaillogs= log file+DECRYPT()//AES is used each owner's log file will copied to respective Emaillogs

9. Email logs send to corresponding mailid of respective owner.

8. IMPLEMENTATION DETAILS.

We propose a novel automatic and enforceable logging mechanism in the cloud. This is a systematic approach to data accountability through the novel usage of JAR files is proposed.In our approach for implementation,we have done a photo selling website where we have applied our new concepts.We use java as the development platform and SQLyog as the database.In this case photos are the data and kept in the corresponding jar file.As the user view or download the photos ,these will be recorded in the lo

gfile.This log file is encrypted by the AES algorithm. We have planned to create a test environment such that where we will host this website in the Amazon cloud.By this a realtime testing can be performed.

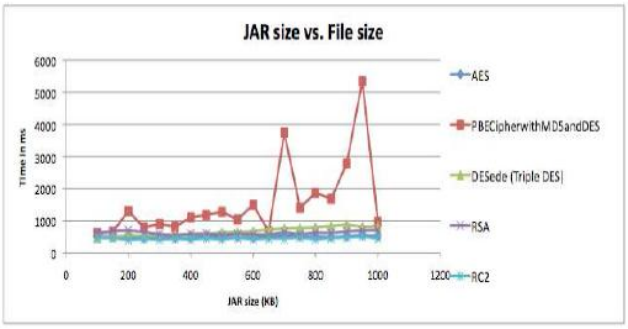

Figure2. Jar file usage.

9. RESULT ANALYSIS.

In our approach we have proposed a concept of one time password at the uploading time. One-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources.And also logfile is protected with the AES algorithm.Which have a strong keylength which make any type hacking is very difficult. Also here the log file mechanism is very effective,where the owner could get it either by a logpush or logpull.And also in our approach jar file is created dynamically ,for each owner in the cloud and in further data will be uploaded to that jar file.Which will help to reduce the heavy network traffic load.

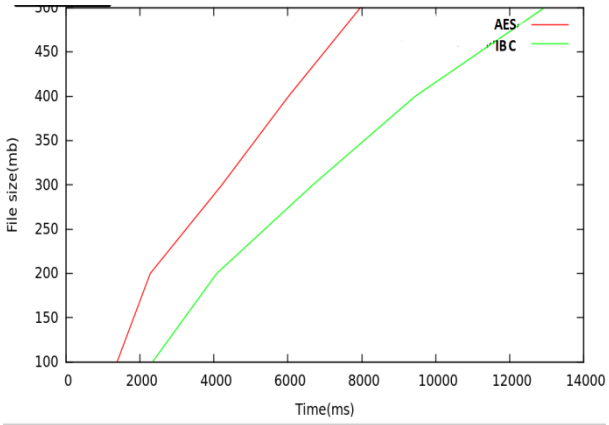

Figure 3. Comparison Graph

10. CONCLUSION AND FUTURE WORK

To summarize, the cloud provides many options for the everyday computer user as well as large and small businesses. It opens up the world of computing to a broader range of uses and increases the ease of use by giving access through any internet connection. However, with this increased ease also come drawbacks. You have less control over who has access to your information and little to no knowledge of where it is stored. You also must be aware of the security risks of having data stored on the cloud. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection. To minimize these problems we have some novel approaches such as a log file concept and its security.We also used one time password concept with the cloud.In the future, we plan to refine our approach with obtaining an encrypted format for the jar file. Also to try to obtain the file integrity checking with this approach. Another enhancement area is application of steganography with the cloud[5].

REFERENCES

[1] Cloud Computing Basics.Association of information technology professionals.

[2] Ensuring Distributed Accountability for Data Sharing in the Cloud Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin

[3] Distributed Accountability for Data Sharing in Cloud. International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012

[4] One Time Password for Multi-Cloud Environment**.** International Journal of Advanced Research in Computer Science and Software Engineering.

[5]. Cloud Computing Security With Steganography and Cryptography AES Algorithm Technology. World Research Journal of Computer Architecture Volume 1, Issue 1, 2012, pp.-11-15. Available online at http://www.bioinfo.in/contents.

[6] Introduction to Cloud Computing architecture White Paper1st Edition, June 2009

[7] B.Crispo and G.Ruffo, "Reasoning about Accountability within Delegation" Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001..

[8] Addressing cloud computing security issues Dimitrios Zissis ∗, Dimitrios Lekkas Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece.

[9] http://en.wikipedia.org/wiki/jar file format.

[10] Decentralized Trust Management and Accountability in Federated Systems ,Brent N. Chun Intel Research Berkeley Andy Bavier Princeton University Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.