IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

Enhancing Security and Reducing Size of Jar File for Data Sharing in Cloud Computing

V. Suresh[1], G. Kanagaraj[2], T. Primya[3], G. Selva Priya[4]

Assistant Professor/CSE, Dr. N. G. P Institute of Technology, Coimbatore [1, 3, 4]

Assistant Professor/CSE, Kumaraguru College of Technology, Coimbatore [2]

Abstract: Cloud Computing is a highly scalable service to be easily consumed over the Internet. A major feature of the Cloud service is the user's data are processed from remote machines. So the users have fears about losing control of their data. We provide a highly decentralized information accountability framework called CIA. CIA is used to keep track of the usage of the users' data in the Cloud System. The JAR programme is used to create dynamic and travelling object, and used to check that any access to user's data will trigger an authentication and automated logging to JAR. Distributed auditing mechanisms are used to provide strength to user's control. The JAR authentication allows the developer to implement powerful applications that they can modify the code and audit the code of the copied code by the attacker.

Keywords: Cloud Information Accountability Framework, JAR Authentication, JAR Files.

I. INTRODUCTION

Cloud Computing user satisfaction is depends upon the security level of users data. Cloud Computing is classified into two types are Services offered and location. Cloud Computing offers three services are : IaaS- Infrastructure as a Service, PaaS- Platform as a Service, and SaaS- Software as a Service. Public Cloud, Private Cloud, hybrid Cloud and community Cloud are the types of Cloud Computing classification depends on location. Cloud computing is a next generation architecture.

Cloud system contains many number of storage servers. Storing data in a third party system causes many problems in data confidentiality. There are some encryption schemes are used to keep the data as confidential. But the encryption schemes are support limited operations. Accountability is used to find the people who is responsible for policy violation. Accountability is mainly used for security.

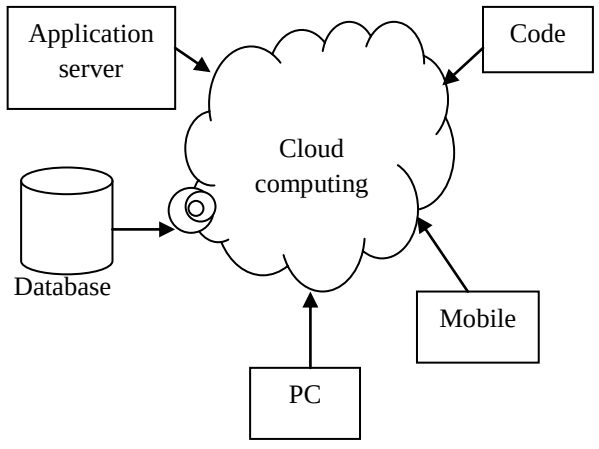

Figure 1: Cloud Computing

Identity Based Encryption(IBE) algorithm is used to encrypt the log records. The Time of access of a data is to be recorded in log record by using Network Time Protocol (NTP).Cloud Information Accountability Framework is used to track the users data usage. This is a best method to provide security to the users data. This framework will record the logs of data usage. CIA is also used to allow the data owner to provide access control to the data. Data owner can audit the log records by using two methods are push mode and pull mode.

Push mode is used to send the log records to data owner periodically. Pull mode is used to retrieve the log records whenever needed. Fig 1 describes the architecture of Cloud Computing. The Cloud Service Provider can be accessed from mobile, pc, laptop etc. CIA framework contains two components are Logger and Log harmonizer.

Logger is used to encrypt the log records using public key and send to the log harmonizer. The log harmonizer is responsible for auditing purpose and used for decrypting the log records which is received from logger.

II. LITERATURE SURVEY

The distributed system supports secure and robust storage, retrieval. Here the user can forward their data from one storage server to another storage server without retrieving the data. Data robustness is a main concept in security.

One way for data robustness is replicate the data. The data are replicated and stored in different storage servers. A decentralized code is used to compute a codeword symbol for each message or data. The process is encode a message and split into n tasks of generating codeword symbol. It is

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

suitable for distributed storage system. The stored messages are encrypted and encoded. At the time of retrieval key servers query the storage servers. [2]

Auditing is a process of verification. There are two types of auditability are private auditability and public auditability. Private auditability is higher efficiency scheme. Public auditability allows anyone to verify.

The data owner does not have the time to verify the data access. So they delegate their work of monitoring data usage to a TPA-Third Party Auditor. Here the TPA can act as a verifier. The data owner can provide block operations or access control on data such as modification, insertion, deletion. [3]

Identity Based Encryption scheme is used to encrypt the log records. It contains four steps are 1.setup 2.Extract 3.Encrypt 4.Decrypt

Setup is used to generate parameters and master key. Extract is used to generate the private by using master key. Encrypt is used to encrypt the log records by using public key. Decrypt is used to decrypt the messages using private key.

Setup takes a parameter S and returns pa and master key. Pa is a system parameter.
Extract takes the input parameter pa, master key and returns a private key.
Encrypt takes pa, ID and returns cipher text C.
Decrypt is used to decrypt the message. It takes parameter pa, C and private key then returns M.[7]

Accountability is a mechanism of verifying authorization policies. The accountability system contains power of auditor, Efficiency of audit protocol. It is a after-the-fact verification means audit the log records.

These log records are used by auditor to find dishonest principles and violation of security policy. There are two contributions are an operational model for accountability and auditors are considered as internal agents. Second is accountability system design and validation of auditors. [9]

The distributed storage auditing mechanism and erasure coded data. It is used to audit the cloud storage and misbehaving error identitification. Data error is identified as fast and dynamic data support is used to maintain storage priority even the user modify, delete the data. Lightweight is used to perform the user operations in a minimum time. [5]

TCPA technologies are used here. TCPA is a mechanism to check the integrity. It can be used to check the receivers platform whether it a trusted computing platform or not. Here the TA- Trusted Authority will issue the decryption key. [10]

Accountability is a main advantage in cloud computing. The problem in accountability is fraud occurs. Here a prototype audit system is used named as DRAGOON.

It is a hashing technique that is used to support accountability for finding error occurs.[11] Audit log is used to find the malfunction behaviours. It is a main process in a accountability.[4]

III. PROBLEM STATEMENT

The fear of data loss is the main issue in cloud computing. So the CIA framework was implemented [1]. But there is no jar authentication.

Here we proposed jar authentication, It will provide more security to the jar file which is contains the data, certificate, encrypted key. From this authentication can prevent the hacking of jar files.

IV. JAR FILES AND AUTHENTICATION

JAR stands for Java Archives. It used to reduce file size and can put many files as a compressed format. It contains a manifest file. Vendor name, product version, data of creation of product. Generally JAR files are like as RAR files. In our system data owner will put their data as a JAR file then sends to Cloud Service Provider. The JAR file contains Data, Log files, encrypted key. We can create and extract the Jar file.

The extraction of a Jar file done by using the following command.
jar xf filename
X-specifies Extract and f-specifies file. Filename specifies the jar file which we want to extract.
The creation of Jar file by using following command.
jar cf filename

Log records which is having in jar file contains the following fields are ID, Acknowledgement, Time of creation, Location. In our system Jar file classified as two types are Inner jar and outer jar. The use of outer jar is authentication of entities which want to access the data stored in jar file created by data owner. The inner jar contains the encrypted data and class file to write log records. IBE key pair is used for encrypting log records.

Our system is JAR authentication which is used to provide more security to jar files. Authentication is provided as follows signed application descriptor file is used to authenticate the jar file. It contains ADF,DDF and developers certificate, file hash.

Application descriptor file is used to check the client system whether it is having sufficient resources or not. Developer descriptor file is used to specify the access control. The file hash is the result of cryptographic method. More than one hash file is used in a signed ADF.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

V. FLOW CHART

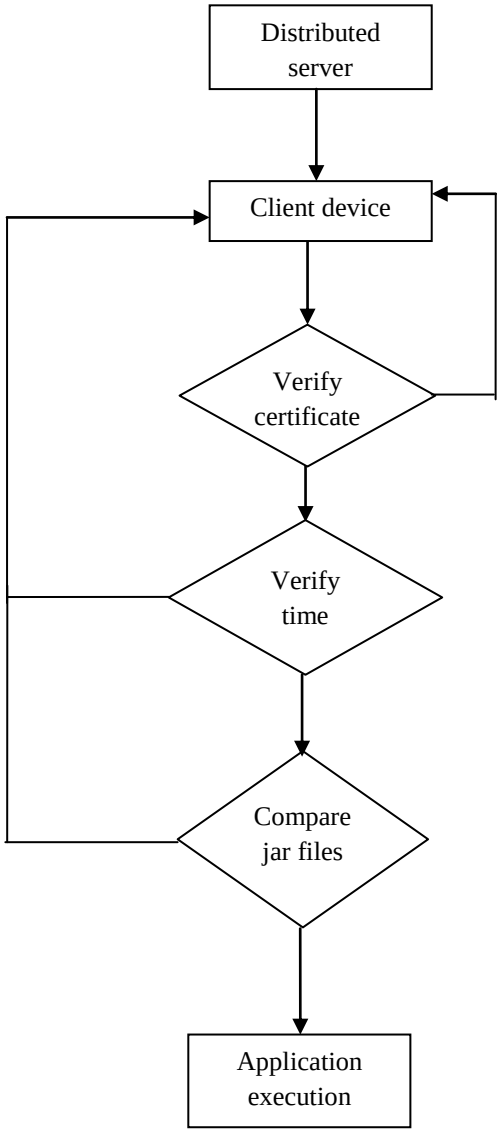

Figure 2.Data flow Diagram

The signed ADF is created and stored in a distribution server. The client sends a request to a distribution server for a specified application. The server first transmits signed ADF for a specified application. After receiving signed ADF client verifies the developers certificate with its authority's public key. Here two types of hash of jar file will be produced. The hash of jar file produced in client device compared with hash of jar file which is received in a signed ADF. If both are match then the client loads the application for execution.

The certificate is within 100-500bytes. The file hash is above 20bytes. The DDF is within 100-200bytes. The ADF maybe 100-200bytes. Here the security is provided to client device with a set of keys such as certificate authority key, time stamp root key. Figure 2 describes the network client device is a client sends a request to server for the application. The corresponding signed ADF is downloaded and checks the ADF,DDF, developers certificate, file hash. The hash of jar file in client device and the hash of jar file which received are compared. If both are same, after that only the application will be executed.

VI. REDUCING JAR FILE SIZE

Jar file is a compressed file format. Generally the logger component contains nearly 10 files. The size of that is 3.5MB to 4MB. It takes more time to store the files in CSP. So it made as a Jar file and compressed into 200KB to 1MB. Generally the Lempel-Ziv algorithm is used to compress a file. It is a lossless compression. Lempel-Ziv algorithm takes linear time to encoding and decoding.

VII. SERVER COLLISION AVOIDANCE

Data owner saves the data in Cloud service provider. The main issue in Cloud Computing is data loss. The data owner have fear about the data recovery after the data loss because of server crash or server collision. The data which is to be stored in CSP. Then it is converted into a encrypted file and stored in another server. Data owner can be retrieve the data by using the encrypted key.

VIII.RESULTS & DISCUSSIONS

Security Level is increased compare to existing system and the time taken to download the Jar file is minimized.

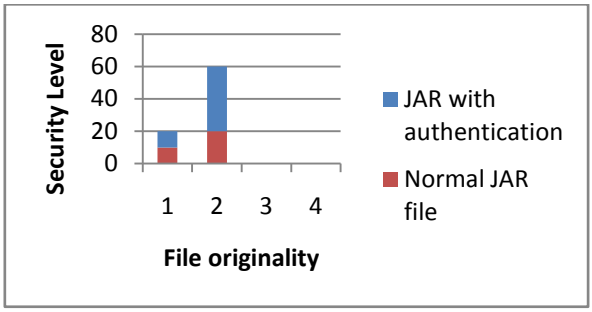

Figure 3 Comparing Security level

The security level of data is showed in above graph. The file originality is increased in our system and the security level also increased.

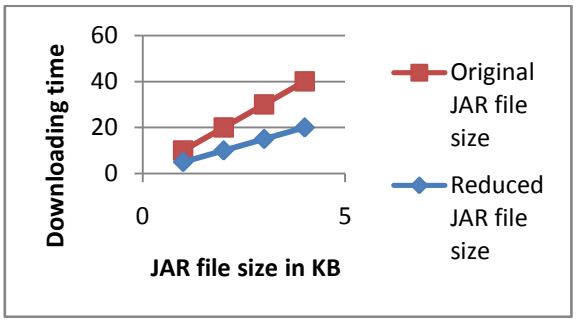

Figure 4 Reduced jar file size with normal jar file

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 8, August 2016

The jar file size is reduced compared to existing system. So the downloading time is reduced.

VI. CONCLUSION & FUTURE WORK

Data access to be tracked by using CIA framework. Then Log records are sent to data owner for auditing purpose. The data is stored as jar file in Cloud Service Provider. Jar file authentication is used to check the original Jar file which is provided by data owner. The file size will be within 1MB. So jar files are used to reduce the file size as a compressed file format. Jar file authentication is implemented for jar file security which is contains data.
In Future work we are planned to provide more security by using various kinds of authentication like as password checking, user verification.

REFRENCES

[1] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, “Ensuring Distributed Accountability for Data Sharing in the Cloud” vol. 9, no. 4, july/august 2012
[2] Hsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, IEEE ,"A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding" , IEEE transactions on parallel and distributed systems, vol. 23, no. 6, june 2012.
[3] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE,Wenjing Lou, Senior Member, IEEE, and Jin Li ,“Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”
[4] Anupam Datta, Dilsun Kaynar, Divya Sharma, Arunesh Sinha,"Poster: Defining Accountability using Causation and Evidence" vol. 367, no. 1-2, pp. 33–56, 2006.
[5] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member, IEEE,"Toward Secure and Dependable Storage Services in Cloud Computing". IEEE transactions on services Computing, vol. 5, no. 2, May 1,2000.
[6] Sneha Prabha Chandran and Mridula Angepat,"Cloud Computing: Analysing the risks involved in Cloud Computing environments" International conference on Information systems, Technology, and Management, Thailand, March, 2010.
[7] Weil Pairing Dan Boneh Matthew Franklin, "Identity-Based Encryption" april 2002.
[8] Brent N. Chun Andy Bavier,"Decentralized Trust Management and Accountability in Federated Systems" June 2009.
[9] Radha Jagadeesan1, Alan Jeffrey, Corin Pitcher1, and James Riely,"Towards a theory of accountability and audit " may 2010.
[10] Marco Casassa Mont, Siani Pearson, Pete Bramhall,"Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services" , Jan 31,2005.
[11] Kyriacos E. Pavlou and Richard T. Snodgrass, "Achieving Database Information Accountability in the Cloud" Tucson, AZ 85721–0077, USA, 2002.
[12] Q. Wang, K. Ren, W. Lou, and Y. Zhang,"Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance " april 2008.
[13] Trusted Java Virtual Machine IBM, http://www.almaden.ibm.com/cs/projects/jvm/, 2012.
[14] http://www.wikinvest.com/concept/Cloud_Computing
[15] Comparison Of Cloud With other Computing "http://www.ibm.com/developerworks/web/library/wa-Cloudgrid/"