ISSN 2277-3061

Secure Distributed Accountability Framework for Data Sharing in Cloud Environment

Vikas Lonare[1], J.N. Nandimath[2]
[1] ME Computer Student, Computer Department, SKNCOE, Pune
[2] Professor, Computer Department, SKNCOE, Pune

ABSTRACT

Cloud computing is used to provide scalable services which are easily used over the internet as per the requirement. A major feature of the cloud services is that user's data are remotely processed in unknown machines that users do not know or users are not operating these machines. While using these services provided by cloud computing, users fear of losing their own data. The content of data can be financial, health, personal. To resolve this problem, we use information accountability in decentralized format to keep track of the usage of the user's data over the cloud. It is object oriented approach that enables enclosing our logging mechanism together with user's data and apply access policies with respect to user's data. We use JAR programming which provides the dynamic and traveling object functionality and to track any access to user's data will call authentication and automated logging mechanism to the JAR files. Each access to user's cloud data will be getting recorded in separate log file. To provide robust users control, distributed auditing functionality is also provided to track the usage of data.

The proposed system also provides the authentication mechanism using external channels and also makes a log of user details from which the cloud data is accessed. Only data owner can retrieve the detail log of his data as per requirement. Data owner will provide the type of access to his data and based on that, authorized data user can access the data over the cloud environment.

General Terms/Keywords

Cloud Computing; Encryption; Decryption; Cloud Service Provider; JAR; Authentication; Key Generation; Uploading and Downloading; Data Sharing.

Academic Discipline and Sub-Disciplines

Cloud Computing and Data Security

SUBJECT CLASSIFICATION

Secure Framework for Data Sharing in Cloud

TYPE (METHOD/APPROACH)

Research Work

1. INTRODUCTION

This paper proposes a model to provide strong security mechanism for Authentication, Authorization and Accountability of data sharing in the cloud environment. In the 1960s, J.C.R. Licklider introduced the term intergalactic computer network at the Advanced Research Projects Agency. This concept served to introduce the concept that the world came to know as the Internet. The term cloud originates from the telecommunications world of the 1990s, when providers began using Virtual Private Network (VPN) services for data communication. VPNs maintained the same bandwidth as networks with considerably less cost. These networks supported dynamic routing, which allowed for a balanced utilization across the network and an increase in bandwidth efficiency, and led to the coining of the term telecom cloud. Cloud computing premise is very similar in that it provides a virtual computing environment that dynamically allocated to meet user needs. From a technical perspective, cloud computing includes service oriented architecture (SOA) and virtual applications of both hardware and software. Within this environment, it provides a scalable services delivery platform. Cloud Computing shares its resources among a cloud of service consumers, partners, and vendors. By sharing resources at various levels, this platform provides various services, such as an infrastructure cloud (for example, hardware or IT infrastructure management), a software cloud (Such as software, middleware, or traditional customer relationship management as a service), an application cloud (application, UML modelling tools, or social networks as a service), and a business cloud for instance, business processes as a service. 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.

2. RELATED WORK

Smitha S, Dan Lin proposes a novel highly decentralized information accountability framework [1] to keep track of the actual usage of data in cloud using JAR files. They have used oblivious hashing and SAMPL authentication. They have implemented the Push-Pull log mode. Qian Wang, Cong Wang present third party auditor scheme in cloud computing using RSA and Bilinear Diffie-Hellman techniques [2]. Parikshit Prasad, R Lal present a system in which data classification done by Owner before storing data [3]. Data categorized on the basis of Confidentiality, Integrity and Availability based on the Classification Algorithm. P L Rini, Anand N Provides innovative approach for automatically logging and auditing mechanism using BASE64 encoding algorithm [6] to protect the data from attackers.

3. PROPOSED MODEL

3.1 Motivation

The cloud user’s logging should be decentralized in order to adapt to the dynamic nature of the cloud environment. Cloud should use minimal infrastructural support from any server operations. Every access to the user’s data should be correctly and automatically logged so that data integrity can be verified. Recovery mechanisms are also desirable to restore damaged files caused by technical problems. System should provide mechanism to use dynamic password using external channel to provide strong authentication.

3.2 Proposed System

A novel highly decentralized information accountability framework to keep track of the actual usage of the user’s data in the cloud. An object-centered approach that enables enclosing our logging mechanism together with user’s data and access policies. JAR programmable capabilities to both create a dynamic and traveling object. Ensure that any access to user’s data will trigger authentication and automated logging local to the JARs with distributed auditing mechanisms. The overall CIA framework, combining data, users, logger and the logging should be decentralized in order to adapt to the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled, and require minimal infrastructural support from any server. Every access to the user’s data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity that accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed. Log files should be reliable and tamper proof to avoid illegal insertion, deletion, and modification by malicious parties. Recovery mechanisms are also desirable to restore damaged log files caused by technical problems. Log files should be sent back to their data owners periodically to inform them about the current usage of their data. More importantly, log files should be retrievable anytime by their data owners when needed regardless the location where the files are stored. The proposed technique should not intrusively monitor data recipients systems, nor should it introduce heavy communication and computation overhead, which otherwise will hinder its feasibility and adoption in practice.

3.3 Proposed Architecture Diagram

The proposed architecture consist of Cloud Service provide CSP, Glassfish Server, My SQL Database and related peripherals.

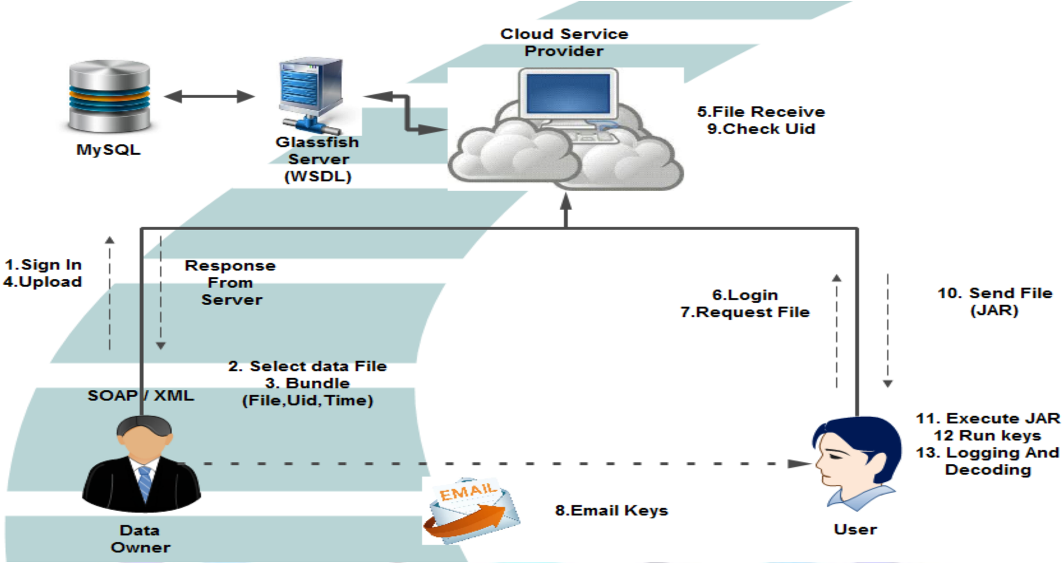

Fig. 1: Architecture of Proposed System

Each JAR file is having two sub parts as Inner JAR and Outer JAR. User's data will be enclosed in JAR file and each JAR file is having own access related properties file. Only the data owner can specify the rules to access the data over the cloud. These rules can be Read, Write, and Update. Advanced Encryption Standard AES algorithm is used to encrypt and decrypt the data over cloud. Some of the applications of AES are still inflexible to various type of cracking techniques, which makes it a better choice even for top secret information. AES data encryption is more scientifically capable and graceful cryptographic algorithm, but its main force rests in the key length. The time necessary to break an encryption algorithm is straightly related to the length of the key used to secure the communication.

3.4 Working

Data owner will login to the system and upload his own file. While uploading file, he will provide the access permission to authorized users. Data owner will receive the private key which is unique to his data only. Further, this private key and data will be getting encrypted and stored in cloud database. Data user will login to the system and user will access only those files for which he is authorized. Once user downloads a file then he needs the private key to open that file. File downloading should be done by authorized users only. This private key will be shared by data owner. User can view the file once he enters the correct private key file. All the activities done by the data user will be get logged and that log file will be retrieve by data owner as per the need. Pure log is used to record every access to the data. The log files are used for pure auditing purpose. Access Log is used for logging actions and enforcing access control. In case 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.

Advanced Encryption Standard

Advanced Encryption Standard (AES) is the current standard for secret key encryption. AES was created by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, replacing the old Data Encryption Standard (DES). The Federal Information Processing Standard 197 used a standardized version of the algorithm called Rijndael for the Advanced Encryption Standard. The algorithm uses a combination of Exclusive-OR operations (XOR), octet substitution with an S-box, row and column rotations, and a Mix Column. It was successful because it was easy to implement and could run in a reasonable amount of time. AES allows you to choose a various type of key like 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.

4. CONTRIBUTION

This system can be used in Cloud environment to provide the strong authentication, authorization and accountability of the user's data. It shows the innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism to enhance the system. This approach allows the data owner to not only audit his data but also enforce strong back-end protection if needed to secure the data. One of the main features of system is that, it enables the data owner to audit even those copies of its data that were made without his knowledge. Robust and Secure data share in cloud using secure external channel authentication and strong encryption and decryption algorithm.

5. ACKNOWLEDGMENT

For proposing this model, we referred the IEEE Transaction paper under the title "Ensuring Distributed Accountability for Data Sharing in the Cloud" IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 4, July/August 2012. This paper contains the proposed system which can be implemented in real time within cloud network.

6. REFERENCES

[1] Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin "Ensuring Distributed Accountability for Data Sharing in the Cloud" IEEE Trans actions On Dependable And Secure Computing, Vol. 9, No. 4, July/August 2012.

[2] 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" IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, May 2011.

[3] Parikshit Prasad, R Lal, "3 Dimensional Security in Cloud Computing" IEEE 2011.

[4] Xiao Zhang, Hong-tao Du , Jian-quan Chen, Yi Lin, Lei-jie Zeng Ensure Data Security in Cloud Storage IEEE 2011.

[5] Yubo Tan , Xinlei Wang Research of Cloud Computing Data Security Technology IEEE 2012.

[6] P L Rini, Anand N “Encoding Personal Information On Data Sharing In Cloud Using BASE64 Algorithm" GRET 2013.

[7] MdMasoom Rabbani, Ilango Paramasivam "Enhancing Accountability for Distributed Data Sharing in the Cloud" IJET Jun-Jul 2013.

[8] P Sobha Rani, P. Suresh Babu "Achieving Information Accountability in Cloud Computing Environment" IJCER April 2013.

[9] Drishya S G, Kavitha Murugeshan "Towards Achieving Secured and Decentralized Accountability in Cloud Computing" IJCTT May 2013.

[10] Prema Mani, Janahanlal P Stephan "Enhanced Accountability Framework for Data Sharing in the Cloud" ICCSE April 2013.