International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2820-2822 ISSN: 2249-6645

A Novel Information Accountability Framework for Cloud Computing

M. Vijaya Lakshmi[1], Syed Sadat Ali[2]
[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*
[2]*Assoc. Professor & Head, Dept. of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*

ABSTRACT: *Cloud computing is an emerging paradigm in the computer industry where the computing is moved to a cloud of computer systems. The cloud computing core concept is, simply, that the vast computing resources that we need will reside somewhere out there in the cloud of computer systems and we will connect to them and use them as and when needed. The difficulty of how to provide proper security as well as privacy protection for cloud computing is very important, and as yet not solved. In this paper we propose a novel approach, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. Unlike privacy protection technologies which are built on the hide-it-or-lose-it perspective, the information accountability focuses on keeping the data usage transparent and trackable. The design of the CIA framework presents substantial challenges, including uniquely identifying CSPs, adapting to a highly decentralized infrastructure, ensuring the reliability of the log, etc. Our basic approach toward addressing these issues is to leverage and extend the programmable capability of the JAR (Java ARchives) files to automatically log the usage of the users' data by any entity in the cloud. Users will send their data along with any policies such as access control policies and logging policies that they want to enforce, that is enclosed in JAR files, to cloud service providers.*

Keywords: *Cloud, CSP, Log file, JAR.*

I. INTRODUCTION

Cloud computing [1] technology is flexible, highly scalable and gives us technology enables services that can be easily consumed over the Internet on as-needed basis. The convenience and efficiency of this approach, however comes with security and privacy risks [2]. Privacy is a key business risk and compliance issue, as it sits at the intersection of the social norms [3]. The advantages of cloud computing is its ability to scale rapidly, share services in a dynamic environment and store data remotely (unknown places). Hence these can become disadvantages in maintaining both privacy and protection to their data to sustain confidence in potential customers. For example, the data processed on the clouds are often outsourced, leading to a number of issues related to accountability, including handling of personal information. Data represents an extremely important asset for any organization, and many users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept secret to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement for cloud environment.

Data confidentiality is not the only security requirement for cloud. Flexible and fine grained access control is also strongly desired in the service oriented cloud computing model. A health care information system on a cloud environment is required to restrict access of protected medical records to eligible doctors and a customer relation management system running on a cloud may allow access of customer information to high level executives of the company only [4]. To solve the security issues in cloud environment; other user cannot read the respective users data without having access. Data owners should not bother about their data, and should not get fear about damage of their data by hackers; there is need of security mechanism which will track usage of data in the cloud. Accountability is necessary for monitoring data usage, in this all actions of the users like sending of file are cryptographically linked to the server, that performs them and server maintain secured record of all the actions of past and the server can use the past records to know the correctness of action. It also provides reliable information about the usage of data and it observes all the records, so it helps in make trust, relationship and reputation. So accountability is for verification of authentication as well as authorization.

II. RELATED WORK

Cloud environment has raised a range of important privacy and security issues [5][6]. Such issues are due to the fact that, in the cloud environment, users' data and applications reside—at least for a certain amount of time—on the cloud cluster which is owned and maintained by the third party. In [7], the authors present a layered architecture for addressing the end-to-end trust management and accountability problem in many federated systems. They mainly consider trust relationships for accountability, along with both authentication and anomaly detection. Researchers have investigated the accountability mostly as a provable property through various cryptographic mechanisms, particularly in the context of electronic commerce [8]. In [9], the authors propose the usage of policies attached to the data and present logic for the accountability data in distributed settings.

In [10], the authors proposed the Proof Carrying authentication (PCA) framework. The PCA includes a high order logic language that allows the quantification over predicates, and focuses on access control for the web services. While related to ours to the extent that it helps maintaining safe, high performance, mobile code, the PCA's goal is highly different from our research work, as it focuses on validating code, rather than monitoring the content. In [11], the authors proposed an approach for strongly coupling content with access control with the help of Identity-Based Encryption (IBE).

III. PROPOSED WORK

The design of our framework presents substantial challenges, including uniquely identifying CSPs, ensuring the reliability of the log, adapting to a highly decentralized infrastructure, etc. Our basic approach toward addressing these issues is to leverage and extend the programmable capability of JAR (Java ARchives) files to automatically log the usage of the users' data by any entity in the cloud environment. Users will send their data along with any policies such as access control policies and logging policies that they want to enforce, that enclosed in JAR files, to cloud service providers. Any access to the data will trigger an automated and authenticated logging mechanism local to the JAR files. As shown in Figure 1, our proposed JAR file consists of one outer JAR enclosing one or more inner JARs. The main responsibility of the outer JAR is to handle authentication process of entities which want to access the data stored in the JAR file. In our context, the data owners may not know the exact CSPs that are going to handle the information. Hence, authentication is specified according to the servers' functionality (which we assume to be known through a lookup service), rather than the server's URL or identification. Log records are generated by using the logger component. Logging occurs at any access to the data in the JAR file, and new log entries are appended sequentially, in order of creation. Each record ri is encrypted individually and then appended to the log file.

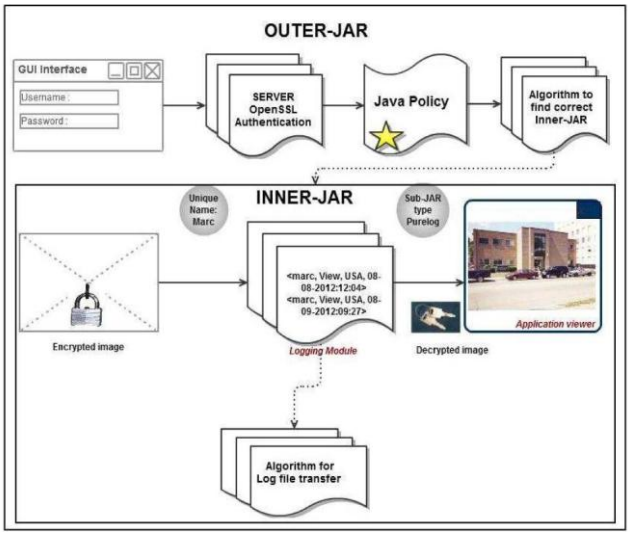

Figure 1: The Structure of the JAR File

Now we propose a new method based on the concept of information accountability. In contrast to the privacy safety is based on the concept of "hide-it-or-lose-it". This information accountability mainly focus on keep the data usage in transparent as well as track able manner. The proposed framework provides end to end accountability in a high dynamically distributed manner. The new innovation in this framework is ability of maintaining lightweight and powerful accountability models, also it integrates the access control methods, usage control and authentication polices.

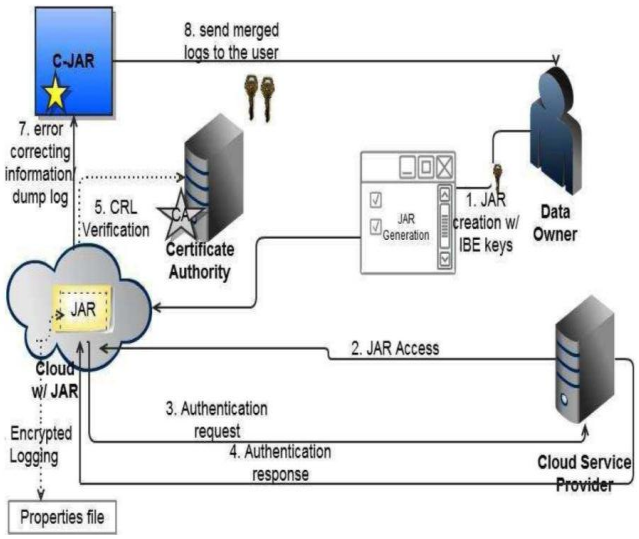

Figure 2: Information Accountability Framework

By means of this, data owners can track not only whether or not the service level agreements are being pleased, but also impose the access and usage control rules based on user needs. Also develop two distinct modes for auditing purpose, they are called as push and pull mode. In push mode, the logs are sporadically pushed to the data owner by using the log harmonizer while in the pull mode refers to another approach whereby the user (or another authorized party) can retrieve the

logs as our needed. The overall proposed framework, which combines data, logger, users and log harmonizer, is shown in the figure 2. Initially, each user creates both private and public keys using Identity-Based Encryption. The user will create a logger component which is a JAR file using this secret key, to store its data elements. The JAR file includes a set of simple access control policies specifying whether and how the cloud servers and possibly the other data stakeholders are authorized to access the content itself. Then, user sends the JAR files to the cloud service provider that he/she subscribes to. To authenticate the CSP to the JAR file, it uses Open SSL(Secure Socket Layer) based certificates, wherein a trusted certificate authority certifies the CSP. In the event that the access is requested by the users, this employs SAML-based authentication, where in a trusted identity provider issues certificates verifying the user's identity based on his user identity. Once the authentication was successful then the service provider will be allowed to access the data enclosed in the JAR file.

IV. CONCLUSION

Cloud computing is receiving a great deal of attention, both in publications and among users, from individuals at home, office to the government. The cloud removes the need for you to be in the same physical location as the hardware that stores your information. A major feature of the cloud services is that user's data are usually processed remotely in unknown systems that users do not own or operate. Data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in various traditional environments. This can be addressed by a novel method, namely Cloud Information Accountability (CIA) framework. In this every access to the data are correctly and automatically logged. Log files should be sent back to their data owners periodically, which are used to inform them of the current usage of their data. More importantly, log files should be retrievable any time by their owners when needed regardless the location where the files are actually stored.

REFERENCES

[1] Jens, F. (September 2008). Defining cloud services and cloud computing. http://blogs.idc.com/ie/?p=190
[2] S.Pearson, "Taking Account of Privacy when Designing Cloud Computing Services".
[3] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud, " Proc First Int'l conf. Cloud Computing, 2009.
[4] ZhiguoWan, Jun'e Liu,Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for flexible and Scalable Access Control in Cloud Computing".
[5] 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.
[6] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), first ed. O' Reilly, 2009.
[7] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.
[8] B. Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.
[9] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.
[10] X. Feng, Z. Ni, Z. Shao, and Y. Guo, "An Open Framework for Foundational Proof-Carrying Code," Proc. ACM SIGPLAN Int'l Workshop Types in Languages Design and Implementation, pp. 67-78, 2007.
[11] M.C. Mont, S. Pearson, and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," Proc. Int'l Workshop Database and Expert Systems Applications (DEXA), pp. 377-382, 2003.