www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume 2 Issue 12, Dec.2013 Page No. 3418-3421

Secure Data Sharing In Cloud by Using CIA

***B. RamaKrishna*[1]*, V.Tirupathi*[2]**

[1]M.Tech in CSE Dept ,
SR Engineering College
Warangal, ANDHRA PRADESH, INDIA
ramakrishnamail4u@gmail.com

[2]Assistant Professor in IT Dept,
SR Engineering College
Warangal, ANDHRA PRADESH, INDIA
thirulu629@gmail.com

***Abstract: Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. To prevent data loss of client an object centered data approach has been proposed. We leverage the JAR programmable capabilities to both create a dynamic and traveling object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, we also provide distributed auditing mechanisms. Cloud Information Accountability (CIA) framework, based on the notion of information accountability*.**

Key Words*: - Cloud Information Accountability (CIA), Cloud Computing, QOS (Quality of Service)*

1. INTRODUCTION

Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles.

The main enabling technology for cloud computing is virtualization. Virtualization generalizes the physical infrastructure, which is the most rigid component, and makes it available as a soft component that is easy to use and manage. By doing so, virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. On the other hand, autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process and reduces the possibility of human errors.

Users face difficult business problems every day. Cloud computing adopts concepts from Service-oriented Architecture (SOA) that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way.

Cloud computing also leverages concepts from utility computing in order to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loops in autonomic computing, allowing services to scale on-demand and to perform automatic failure recovery.

Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

Cloud computing shares characteristics with:

- Client–server model — *Client–server computing* refers broadly to any distributed application that distinguishes between service providers (servers) and service requestors (clients).
- Grid computing — "A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a cluster of networked, loosely coupled computers acting in concert to perform very large tasks."
- Mainframe computer — Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as: census; industry and consumer statistics; police and secret intelligence services; enterprise resource planning; and financial transaction processing.
- Utility computing — The "packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity."
- Peer-to-peer — A distributed architecture without the need for central coordination. Participants are both suppliers and consumers of resources (in contrast to the traditional client–server model).
- Cloud gaming — Also known as on-demand gaming, is a way of delivering games to computers. Gaming data is stored in the provider's server, so that gaming is independent of client computers used to play the game. One such current example would be a service by Online which allows users a certain space to save game data, and load games within the online server.

2. RELATED WORK

2.1 Security and Privacy

2.1.1. Identity management

Every enterprise will have its own identity management system to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own.

2.1.2. Physical and personnel security

Providers ensure that physical machines are adequately secure and that access to these machines as well as all relevant customer data is not only restricted but that access is documented.

2.1.3. Availability

Cloud providers assure customers that they will have regular and predictable access to their data and applications.

2.1.4. Application security

Cloud providers ensure that applications available as a service via the cloud are secure by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires application security measures be in place in the production environment.

2.1.5. Privacy

Finally, providers ensure that all critical data (credit card numbers, for example) are masked and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

2.1.6. Legal issues

In addition, providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

Researchers have investigated accountability mostly as a provable property through cryptographic mechanisms, particularly in the context of electronic commerce. Are preventative work in this area is given by. The authors propose the usage of policies attached to the data and present logic for accountability data in distributed settings. Similarly, Jagadeesan et al. recently proposed logic for designing accountability-based distributed systems.

In Crispo and Ruffo proposed an interesting approach related to accountability in case of delegation. Delegation is complementary to our work, in that we do not aim at controlling the information workflow in the clouds. In a summary, all these works stay at a theoretical level and do not include any algorithm for tasks like mandatory logging.

3. PROBLEM STATEMENT

We aim to develop novel logging and auditing techniques which satisfy the following requirements:

1. 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.

2. Every access to the user's data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity who accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed.

3. 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.

4. Log files should be sent back to their data owners periodically to inform them of 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.

5. The proposed technique should not intrusively monitor data recipients' systems, nor it should introduce heavy communication and computation overhead, which otherwise will hinder its feasibility and adoption in practice.

4. EXISTING SYSTEM

To allay users' concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments.

5. PROPOSED SYSTEM

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, information accountability focuses on keeping the data usage transparent and trackable. Our proposed CIA framework provides end-toend 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. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Associated with the accountability feature, we also develop two distinct modes for auditing: push mode and pull mode. 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.

Our main contributions are as follows:

We propose a novel automatic and enforceable logging mechanism in the cloud.

Our proposed architecture is platform independent and highly decentralized, in that it does not require any dedicated authentication or storage system in place.

We go beyond traditional access control in that we provide a certain degree of usage control for the protected data after these are delivered to the receiver.

We conduct experiments on a real cloud testbed. The results demonstrate the efficiency, scalability, and granularity of our approach. We also provide a detailed security analysis and discuss the reliability and strength of our architecture.

6. CONCLUSION

We proposed innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. Our approach allows the dataowner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge.

7. REFERENCES

[1] S. Oaks, Java Security. O'Really, 2001.

[2] J. Park and R. Sandhu, "Towards Usage Control Models: Beyond Traditional Access Control," SACMAT '02: Proc. Seventh ACMSymp. Access Control Models and Technologies, pp. 57-64, 2002.

[3] J. Park and R. Sandhu, "The Uconabc Usage Control Model,"ACM Trans. Information and System Security, vol. 7, no. 1, pp. 128-174, 2004.

[4] S. Pearson and A. Charlesworth, "Accountability as a WayForward for Privacy Protection in the Cloud," Proc. First Int'l Conf. Cloud Computing, 2009.

[5] S. Pearson, Y. Shen, and M. Mowbray, "A Privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (CloudCom),pp. 90-106, 2009.

[6] A. Pretschner, M. Hilty, and D. Basin, "Distributed Usage Control," Comm. ACM, vol. 49, no. 9, pp. 39-44, Sept. 2006.

[7] A. Pretschner, M. Hilty, F. Schuo¨ tz, C. Schaefer, and T. Walter, "Usage Control Enforcement: Present and Future," IEEE Security & Privacy, vol. 6, no. 4, pp. 44-53, July/Aug. 2008.

[8] A. Prets chner, F. Schuo¨ tz, C. Schaefer, and T. Walter, "Policy Evolution in Distributed Usage Control," Electronic Notes TheoreticalComputer Science, vol. 244, pp. 109-123, 2009.

[9] NTP: The Network Time Protocol, http://www.ntp.org/, 2012.

[10] S. Roman, Coding and Information Theory. Springer-Verlag, 1992.

[11] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1993.

[38] T.J.E. Schwarz and E.L. Miller, “Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage,” Proc. IEEE Int’l Conf. Distributed Systems, p. 12, 2006.

[12] A. Squicciarini, S. Sundareswaran, and D. Li n, “Preventing Information Leakage from Indexing in the Cloud,” Proc. IEEEInt’l Conf. Cloud Computing, 2010.

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

[14] Eucalyptus Systems, http://www.eucalyptus.com/, 2012.

[15] Emulab Network Emulation Testbed, www.emulab.net, 2012.

[16] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing,” Proc. European Conf. Research in Computer Security (ESORICS), pp. 355-370, 2009.

[17] D.J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigen-baum, J.Hendler, and G.J. Sussman, “Information Accountability,” Comm. ACM, vol. 51, no. 6, pp. 82-87, 2008.

[18] Reed-Solomon Codes and Their Applications, S.B. Wicker and V.K.Bhargava, ed. John Wiley & Sons, 1999.

[19] M. Xu, X. Jiang, R. Sandhu, and X. Zhang, “Towards a VMMBased Usage Control Framework for OS Kernel Integrity Protection,” SACMAT ‘07: Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 71-80, 2007.