ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Securable Auditing for Data Sharing in The Cloud

[I]S.Narasimhulu, [II]M.V Prakash
[I,II]Assistant Professor, Dept. of CSE, S.V College of Engineering, Tirupati, AP, India

Abstract
Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. 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. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. To address this problem, in this paper, a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. 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, provide distributed auditing mechanisms. Extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches.

Keywords
Accountability, Data Sharing, CIA Frame Work, Securable Auditing, Trigger Authentication.

I. Introduction

Cloud computing is the access to computers and their functionality via the Internet or a local area network where clients request clouds access from a set of web services that manage a pool of computing resources (i.e. machines, network, storage, operating systems, application development environments, application programs). Requests are dedicated to user until he or she releases them. Cloud computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable and often virtualized resources as a service by cloud. Today, there are a number of notable commercial and individual cloud computing services, including Amazon, Google, Microsoft, Yahoo, and Sales force etc. Users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, they also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to many issues related to accountability, including the handling of personally identifiable information and these fears are becoming a significant obstacle to the wide acceptance of cloud services. Accountability is the obligation to act as a responsible for preserving the personal information of others and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that personal information. Accountability places a legal responsibility on an organization to guarantee that the contracted partners to whom it supplies data are compliant and privacy. 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 can retrieve the logs as needed. A Cloud Information Accountability (CIA) framework based on the notion of information accountability which focuses on keeping the data usage transparent and trackable. CIA framework provides end-to end accountability in a highly distributed fashion that influence and expand the programmable capability of 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, enclosed in JAR files, to cloud service providers. Any access to the data will trigger an automated and authenticated logging mechanism local to the JARs.

II. System Model

A. Data Owner Configuration Phase

In this module every data owner must register their details in the cloud server. And Cloud server establishes the public key and private key access policy using IBE scheme. Finally the cloud server distributes the secret key to the data owner. Cloud server stores the data owner details in the data store as a entity (it is key object model). It is persistence storage

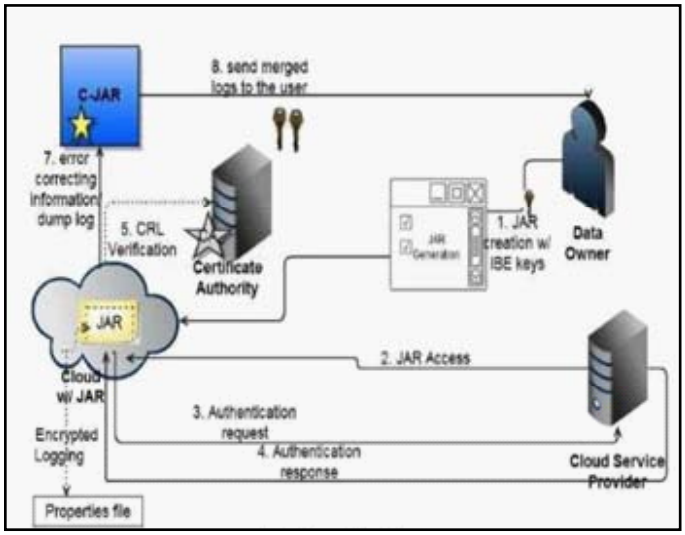

Fig. 1 : Overall Architecture

B. Data Uploading in Cloud Server

After configuration process completed data owner create the log file (it contain configuration details) and encrypt it using the secret key established by the cloud server to the particular data owner. Then load the owner data into encrypted log file. The owner data and log file is bounded or coupled together.

C. User Configuration Phase

In this module every user must register their details and account details in the cloud server. And Cloud server establishes the public key and private key access policy using IBE scheme. Finally the cloud server distributes the secret key to the user. Cloud server stores the user details in the data store as a entity (it is key object

model). When the user request to get the data from the cloud server, the user get data with log file. This log file store the user session details and finally this log file send to data owner.

D. Auditing Phase

In this module log harmonizer is used to perform the auditing work. This is maintained in the data owner. Data owner gets the log file information from the cloud server and user separately and decrypts the log files using the secret keys of data owner, and passes decrypted log files into the log harmonizer. Finally auditing process is conducted.

III. Cloud Scenario

We have a cloud computing scenario as a significance context to describe Electronic Data Sharing Agreements i.e. e-DSAs related policy definitions and their enforcement. The e-DSAs and their automated enforcement are keys to further enable business interactions and information flows within the Cloud, by providing more assurance and control on data where multiple Cloud Service Provider (CSP) available in the Internet. A customer services are supplied by a specific CSP to access online travelling, printing, office applications, etc. To require their access services, customers need to register and disclose personal data, inclusive of address, financial details, etc and to provide the required functionalities, a CSP might need to interact with other Service Providers and share relevant data to enable the business transaction. For example, e-banking services using credit cards buying online may require users account details to be disclosed , e-transactions in order to supply the required service to the customers where it can potentially be analyzed, processed and exchange the information between parties. The key issue is that both the customer and service providers may lose control on data when this data is exchanged between different parties in chains of interactions. Customers might desire to know control details about: How their data should be used; who can access it, etc. (i.e. accountability) ;The purposes for which data can be disclosed to third parties.(i.e. sharing information to other organization);Impose constraints on the retention time, notifications, etc. Similar comments apply to a service provider disclosing information to third parties.

Including privacy preferences on how their personal and confidential data should be handled along with access control and obligation constraints for examples of authorization policies for access control and obligation policies like

Authorization Policies and obligation policies

1. Data of my credit card can be accessed by Service Provider 1(SP1) only for Business Transaction purpose.
2. My email address can be shared with SP2 and SP3 only for business transaction and goods delivery purpose (For businesses: defined legal environment, allowing risk assessments. For individuals: maintenance of societal rights, privacy, and right to time and memory loss but as consumers: defined legal environment Multi party security requirements.)
3. My email address details must not be shared with SP4.

The obligation policies on the users data would be like where I want to be notified by email every time my data is accessed; I want to be notified every time my credit card is disclosed to another Service Provider; I want my data to be deleted after 1 year if not accessed/used.

Interestingly, the stated constraints might need to be enforced by all the entities involved in a chain of data disclosures, e.g. in the example, by the banking Service, the Printing Service, the Flight Booking Service, etc where the customer might change their mind and modify some of their preferences and constraints. These changes should be passing through the chain of disclosures as well. Security in cloud computing consist of security abilities of web browsers and web service structure.

IV. Related Work on Security

In this section we try to highlight the framework suggested by of Marco Casassa Mont, Siani Pearson, Pete Bram hall discussed some problems related with the personal information security. In order to discuss the involved problem, we refer to an e-commerce scenario. By providing damage recovery options mainly: contracts, legal entities, activity logs, defined and agreed transactions .we initially provides personal digital identity and profile information to an e-commerce site in order to access their services, possibly after negotiations about which privacy policies need to be applied . Then the user logs in and interacts with these services: it might happen that in so doing he/she needs to involve other web sites or organizations. The user might be conscious of this or this might happen behind the scenes, for example due to the fact that the e-commerce site interacts with partners and suppliers. The e-commerce site might need to disclose personal data to third parties (such as suppliers, information providers, government institutions etc.) in order to fulfill the specific transaction. This involved e-commerce sites do not necessarily have prior agreements or belong to the same web of trust. Such scenario highlights a few key issues: how to fulfill users' privacy rights and make users be in control of their information. At the same time users' interactions need to be simple and intuitive Privacy and data protection laws that regulate this area do exist but it is hard to monitor them, especially when private information spread across organizations and nations' boundaries. In addition, further complexity arises due to the fact that privacy laws can differ quite substantially depending on national and geographical aspects. For example in US privacy laws restrict what the government can do with personal data but they introduce few restrictions on trading of personally identifiable information private enterprises.

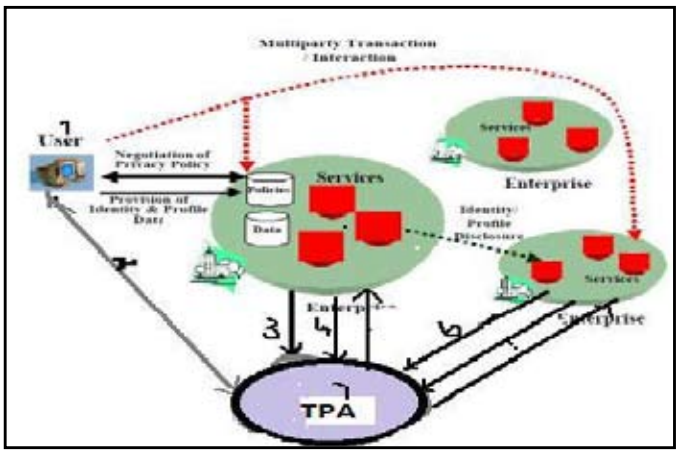

Fig. 2 A scenario where users deal with e-transactions that span across multiple ecommerce sites. In Europe (EU) people can consent to have their personally identifiable information used for commercial purposes but the default is to protect that information and not allow it to be used indiscriminately for marketing purposes.

In this model people Graphical tools locally author their disclosure

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

policies (i.e. sticky polices) in a fine-grained way; Obfuscate their confidential data by directly using these disclosure polices; Associate these policies to the obfuscated data. Some of the above activities can be automated by using predefined policy templates and scripts. Digital packages: containing obfuscated data along with their sticky polices can be provided to requestors such as ecommerce sites. These digital packages might contain a superset of the required information, Selective disclosure of (part of) their contents will be authorized, depending on needs. A requestor has to demonstrate to the Tracing Authority that he/she understands the involved terms and conditions. A Tracing Authority checks trustworthiness of the requestor's credentials and their IT environment accordingly to the disclosure policies.

The owner of the confidential information can be actively involved in the disclosure process by asking for his authorizations or by notifications, according to the agreed disclosure policies. The actual disclosure of any obfuscated data to a request or (for example the e-commerce site) only happens after the requestor demonstrates to a trusted third party – i.e. the "Tracing Authority" - that it can satisfy the associated sticky policies. Disclosures of confidential data are logged and audited by the Tracing Authority In our model nothing prevents the owner of the confidential information from running a Tracing Authority. (8)This increases the accountability of the requestors by creating evidence about their knowledge of users' confidential data. In particular this applies when confidential information is in discriminately disclosed to third parties, as this evidence can be used for forensic analysis. In case a request or sends the obfuscated data package to a third party the same process, described above, applies. Multiple trusted third parties can be used in the above process in order to minimize the risks involved in the management of trust, for example having to rely only on one entity. Once the authentication succeeds, the service provider (or the user) will be allowed to access the data enclosed in the JAR. The accountability in distributed data sharing mechanism with auditing modes and logging mechanism as referred in .

V. Experimental Result

This experiment the time taken to create a log file and then measure the overhead in the system. With respect to time, the overhead can occur at three points: during the authentication, during encryption of a log record, and during the merging of the logs.

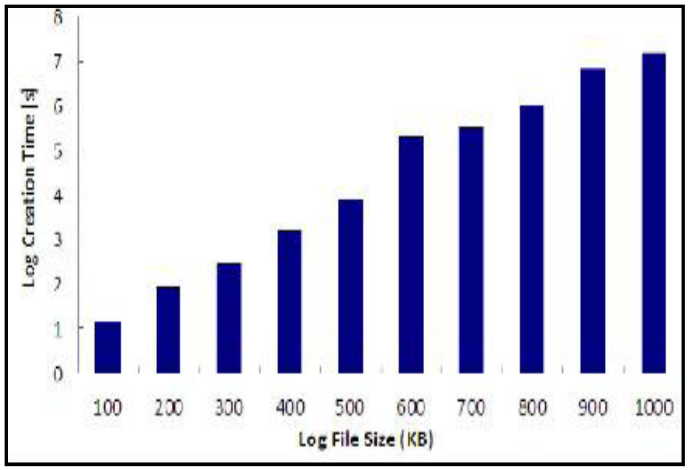

Fig 2: This result shows that time to create log files of different sizes.

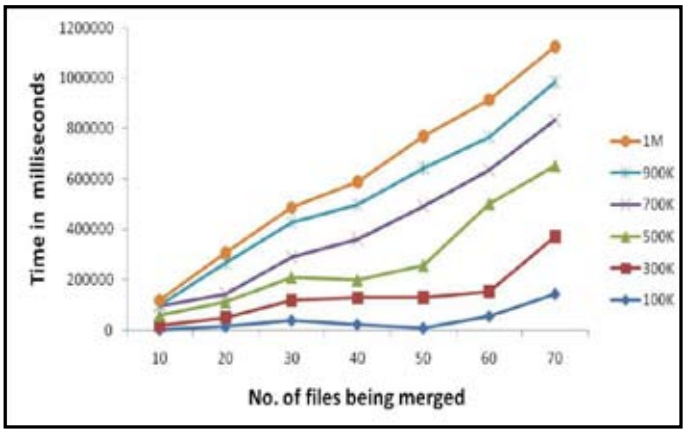

Fig. 3: This result shows that time to merge log files

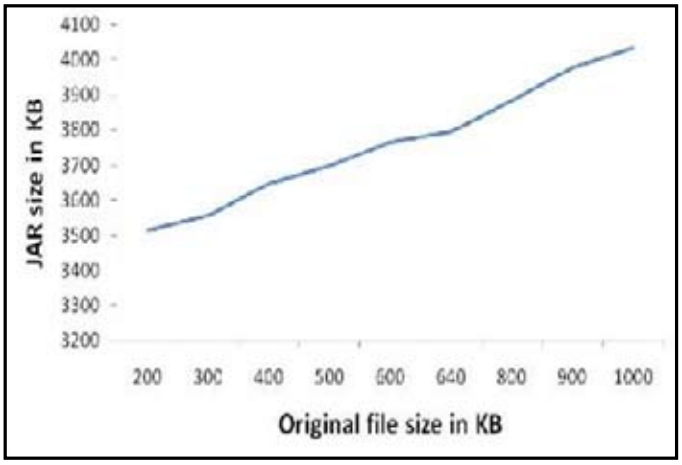

Fig. 4: This result shows that size of the logger component.

VI. Conclusion

It is more and more important to defend and preserve people's privacy on the Internet, against unwanted and unauthorized disclosure of their confidential data. Throughout this paper, the authors have systematically studied and review the security and privacy issues in cloud computing. We propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, we propose an object centered approach that enables enclosing our logging mechanism together with users' data and policies. We have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-preservability). Cloud computing is a new term that is introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the consumers. It has model to protect its data for the business users. An organization used private clouds within its organization to prevent from loss of data.

References

[1] *B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.*

[2] *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.*

[3] *J.W. Holford, W.J. Caelli, and A.W. Rhodes, "Using Self-Defending Objects to Develop Security Aware Applications*

in Java," Proc. 27th Australasian Conf. Computer Science, vol. 26,pp. 341-349, 2004.

[4] 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.

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

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

[7] Sumitha Sundareswaran, Anna C. Squicciarini, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and secure computing, Vol 9. No.4, July/Aug 2012.

[8] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang,"Promoting Distributed Accountability in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2011.

[9] 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.

[10] 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.

[11] 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.

[12] Text Books [1] Cloud Computing, Principles and Paradigms by John Wiley & Sons.

[13] Conference Proceedings[1] Ensuring Distributed Accountability for Data Sharing in the Cloud Author, Smitha Sundareswaran, Anna C.Squicciarini, Member, IEEE, and Dan Lin, IEEE Transactions on Dependable and Secure Computing ,VOL 9,NO,4 July/August 22012 .

[14] Hsio Ying Lin,Tzeng.W.G, "A Secure Erasure Code-Based Cloud Storage System with Secure Data forwarding", IEEE transactions on parallel and distributed systems,2012.

S.Narasimhulu completed his Master of Technology M.Tech in Computer Science and Engineering at Siddharth Institute of Engineering and Technology Puttur, Andhra Pradesh, India. His interest includes Data Mining, Network Security.

M.V.Prakash completed his Master of Technology M.Tech in Computer cience and Engineering at S.V College Of Engineering, Tirupathi, Andhra Pradesh, India. His interest includes Data Mining,