IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 13, Issue 2 (Jul. - Aug. 2013), PP 93-96
www.iosrjournals.org

Cloud Information Accountability Frameworks for Data Sharing in Cloud

[1] C. Madhuri, [2] A. Krishna chaitanya
[1]*CSE Dept, Vardhaman College of Engineering, Hyderabad, India,*
[2]*IT Dept, VCE, Hyderabad, India,*

Abstract: *The ability to hold individuals or organizations accountable for transactions is important in most of the commercial and legal or e-transactions. 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. Where user have everything to be deal on internet on e-transaction to save work and time but we fear for our confidential and individual data is in safe or not, is it been hacked and misused is a fear that stops to use of modern technology. Moreover, users may not know the machines which actually process and host own data. While enjoying the convenience brought by this new technology, end users also start worrying about security of their own personal and important data. Accountability traces every important aspect of any data sharing on data usage in cloud where it accounts every action in the system can be traced back to some entity with assuring the safety and security including the handling of personally identifiable information. In this paper we review the cloud information accountability framework for the data sharing in which procedural and technical solutions are co-designed to demonstrate accountability by the various researchers to resolving privacy and security risks within the cloud and presents a review on new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable framework.*
Keywords*: e-transactions, Accountability, TPA, Tracing Authority.*

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 Salesforce 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 [2] 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 [1], 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.

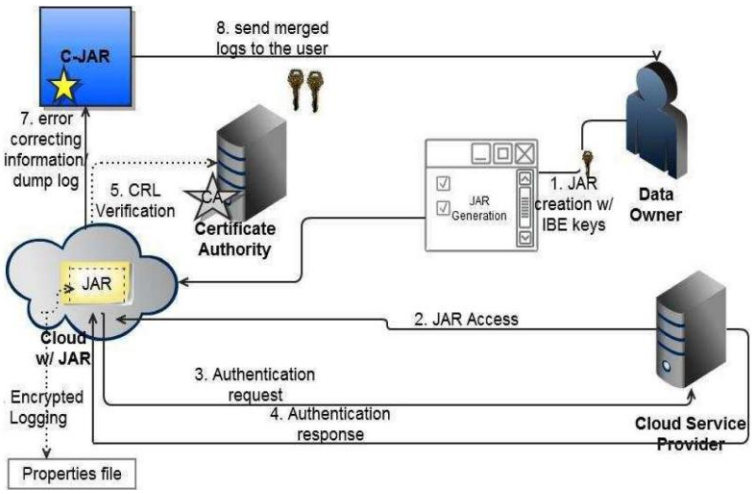

Fig. 1: A framework for cloud computing accountability

Cloud computing has raised a range of important privacy and security issues. The basic idea is that the user's private data are sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The work of A. Squicciarini, S. Sundareswaran, and D. Lin [5] a Java-based approach is provided to prevent privacy leakage from indexing, which could be integrated with the CIA framework proposed in this work since they build on related architectures. We do not rely on IBE to bind the content with the rules. Instead, we use it to provide strong guarantees for the encrypted content and the log files, such as protection against chosen plaintext and cipher text attacks. To its accountability plays a major role in electronic transaction that takes place in reality via internet in our day to day life is explained in his paper with multi party transactions and users confidential data [6].

II. 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 [3]. 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.[7]

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**

- Data of my credit card can be accessed by Service Provider 1(SP1) only for Business Transaction purpose.
- 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.)
- 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.

III. Related Work On Information 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. [3] 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. [7]

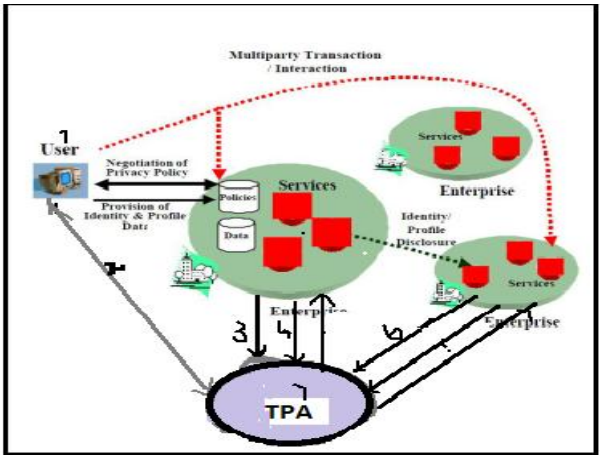

Fig 2 A scenario where users deal with e-transactions that span across multiple ecommerce sites. In Europe (EU) people can consent to have their personally identifiable information used for commercial purposes but the default is to protect that information and not allow it to be used indiscriminately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

In this model people Graphical tools (1) locally author their disclosure 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: (2) 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 (3) 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 (4) accordingly to the disclosure policies. The owner of the confidential information can be actively involved in the disclosure process (5) by asking for his authorizations or by notifications, according to the agreed disclosure policies. The actual disclosure (6) of any obfuscated data to a requestor (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[3]. Disclosures of confidential data are logged and audited by the Tracing Authority (7).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 requestor 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 [6].

IV. 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] S. Sundareswaran, A. Squicciarini, D. Lin, " Distributed Accountability for Data Sharing in the Cloud," *Proc. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No.4,* Aug. 2012.
[2] S. Pearson, "Towards Accountability in the Cloud ," *Proc. IEEE Internet Computing,* pp. 64-69, 2011
[3] Mr. Marco Casassa Mont, Siani Pearson, Pete Bramhall , Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services HPL-2003-49 March 19th , 2003.
[4] Siani Pearson and Andrew Charles worth " Accountability as a Way Forward for Privacy Protection in the Cloud".
[5] A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing Information Leakage from Indexing in the Cloud," *Proc. IEEE Int'l Conf. Cloud Computing,* 2010.
[6] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," *Proc. IEEE Int'l Conf. Cloud Computing,* 2011.
[7] Shraddha B. Toney, Sandeep U.Kadam "Cloud Information Accountability Frameworks for Data Sharing in Cloud." 13th May 2012.