ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

A Prospective Study on Distributed Accountability and Trusted Data Sharing in Cloud Computing

[1]G.S.Suriyakumar , [2]K.Manoj kumar, [3]J.Muruganth , [4]E.Sivaraman
Department of Computer Science and Engineering, Nandha Engineering College, Erode
[5]S. Maheswari,
Department of Computer Science and Engineering, Nandha Engineering College, Erode
[1]UG Scholar, [2] Associate Professor

[1]E-Mail:manojajith95@gmail.com

ABSTRACT :

The key barrier to widespread uptake of cloud computing is the lack of faith in clouds by potential customers. While preventive controls for security and privacy measures are actively being researched, there is still little focus on detective controls related to cloud distributed accountability and audit ability. The complexity resulting from the sheer amount of virtualization and data distribution carried out in current clouds has also revealed an urgent need for research in cloud accountability, as has the shift in focus of customer concerns from server health and utilization to the integrity and safety of end-users' data. This paper discusses key challenges in achieving a trusted cloud data sharing through the use of detective controls, and presents the trust cloud framework, which addresses accountability in cloud computing via technical and policy- based approaches.

Keywords- trust in cloud computing, logging, audit ability, accountability, data provenance, continuous auditing and monitoring, governance.

1.INTRODUCTION:

Cloud computing requires companies and individuals to transfer some or all control of computing resources to cloud service providers (CSPs). Such transfers naturally pose concerns for company decision makers. In a recent 2010 survey by Fujitsu Research Institute on potential cloud customers, it was found that 88% of potential cloud consumers are worried about who has access to their data, and demanded more awareness of what goes on in the backend physical server. Such surveys demonstrate the urgency for practitioners and researchers to quickly address obstacles to trust. While risks can be greatly mitigated via preventive

controls for privacy and security (e.g. encryption, access control based on ID profiling, etc), they are not enough. There is a need to complement such measures with equally important measures that promote transparency, governance and accountability of the CSPs.

This was also identified by The European Network and Information Security Agency (ENISA)'s cloud computing risk assessment report which states that the 'loss of governance' as one of the top risks of cloud computing, especially Infrastructures as a Service (IaaS). Despite audit ability being a crucial component of improving trust, current prominent providers (e.g. Amazon EC2/ S3 , Microsoft Azure are still not providing full transparency and capabilities for the tracking and auditing of the file access history and data provenance of both the physical and virtual servers utilized Currently, users can at best monitor the virtual hardware performance metrics and the system event logs of the services they engage. The cloud computing research community, particularly the Cloud Security Alliance, has recognized this. In its Top Threats to Cloud Computing Report (Ver.1.0) it listed seven top threats to cloud computing: Insecure application programming interfaces, Malicious insiders, Shared technology vulnerabilities, Data loss , Account, service and , Unknown risk profile.

2.TRUST IN CLOUDCOMPUTING:

While there is no universally accepted definition of trust in cloud computing, it is important to clarify its components and meaning. In dictionaries, trust is generally related to "levels of confidence in something or someone" . Hence we can view trust in the cloud as the customers' level of confidence in using the cloud, and try to increase this by mitigating technical and psychological barriers to using cloud services. For more analysis cloud computing, see

To best mitigate barriers to confidence, we need to understand the main components affecting cloud trust: Security -Mechanisms (e.g. encryption) which make it extremely difficult or uneconomical for an un-authorized person to access some information. Privacy -Protection against the exposure or leakage of personal or confidential data (e.g. personally identifiable information (PII)). Determines the level of access to system resources attributed to a particular authenticated user The principle of access control determines who should be able to access what .For Example, we can specify that user XYZ can view the records in a database, but cannot update them. However, user PQR might be allowed to make updates as well. Access control mechanism can be used to ensure this. Using cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with cloud providers.

PREVENTIVE VERSUS DETECTIVE CONTROLS:

Trust components can be also classified as Preventive Controls or Detective Controls. Preventive controls are used to mitigate the occurrence of an action from continuing or taking place at all (e.g. an access list that governs who may read or modify a file or database, or network and host firewalls that block all but allowable activity). Detective controls are used to identify the occurrence of a privacy or security risk that goes against the privacy or security policies and procedures (for example, an intrusion detection system on a host or network, or security audit trails,

logs and analysis tools). In addition, there are corrective controls,(e.g. an incident management plan) which are used to fix an undesired result that has already occurred. This paper focuses on detective controls for cloud computing. Despite the lack of direct ability to stop irregularities from occurring, these controls are very important. They act as psychological obstacles to go against policies or procedures in the cloud, and also serves as a record for post- mortem investigations should any non-compliance occur. They act as in a similar way as speed cameras do for traffic control: the presence of speed cameras will deter law-abiding citizens from speeding, but their presence cannot prevent speeding from taking place. Detective controls hence complement preventive controls. A combination of usually required for reasonable protection.

III.THECLOUDACCOUNTABILITYLIFECYCLE

Figure 1. The Cloud Accountability Life Cycle (CALC)

The discussions in Section III show not only the scale and urgency of achieving cloud accountability but also exposed the need for reduction of complexity. Having an awareness of the key accountability phases will not only simplify the problem, but also allow tool makers and their customers to gauge the comprehensiveness of tools (i.e. whether there are any phases not covered by a tool). A classification of the different phases may also help researchers to focus on specific research sub-problems of the large cloud account ability problem. These phases are collectively known as the Cloud Accountability Life Cycle (CALC) which consists of the following seven phases(seeFigure1):

POLICY PLANNING:

CSPs have to decide what information to log and which events to log on-the-fly. It is not the focus of this paper to claim or provide an exhaustive list of recommended data to be logged. However, in our observation, there are generally four important groups of data that must be logged: Event data – a sequence of activities and relevant information, Actor Data – the person or computer component (e.g. worm) which trigger the event, Timestamp Data – the time and date the event took place, and Location Data – both virtual and physical (network, memory, etc) server addresses at which the event took place.

SENSE AND TRACE:

The main aim of this phase is to act as a sensor and to trigger logging whenever an expected phenomenon occurs in the CSP's cloud (in real time). Accountability tools need to be able to track from the lowest-level system read/write calls all the way to the irregularities of high-level workflows hosted in virtual machines in disparate physical servers and locations. Also, there is a need to trace the routes of the network packets within the cloud.

LOGGING:

File-centric perspective logging is performed on both virtual and physical layers in the cloud. Considerations include the lifespan of the logs within the cloud, the detail of data to be logged and the

location of storage of the logs. . It may in some cases be necessary.

Safe-keeping: After logging is done, we need to protect the integrity of the logs to prevent unauthorized access and ensure that they are tamper-free. Encryption may be applied to protect the logs. There should also be mechanisms to ensure proper backing up of logs and prevent loss or corruption of logs.

AUDITING:

Logs and reports are checked and potential irregularities highlighted. The checking can be performed by auditors or stakeholders. If automated, the process of auditing will become 'enforcement'. Automated enforcement is very feasible for the massive cloud environment, enabling cloud system administrators to detect irregularities more efficiently.

THE TRUSTCLOUDFRAMEWORK:

Provenance Logger:

In order to enable reasoning about the origins, collection or creation, evolution, and use of data, it is essential to track the history of data, i.e., its provenance. Provenance information has been described as 'the foundation for any reasonable model of privacy and trust' in the context of the Semantic Web and we believe it to be similarly central to trust in Cloud Computing. It enables validation of the processes involved in generating/obtaining the data and the detection of unusual behavior. While these advantages are very promising, corresponding challenges are equally difficult to address/overcome. Common challenges include efficiently and effectively managing the sheer amount of provenance data that has to be maintained; ensuring consistency and completeness of provenance data; detecting malicious users who attempt to falsify provenance data; protecting data owner as well as data providers from exposing sensitive, confidential, proprietary or competitively important information indirectly through provenance logs; enabling efficient querying of provenance data; etc.

OPERATING SYSTEMS(OS):

OS system and event logs are the most common type of logs associated with cloud computing at the moment. However, these logs are not the main contributing factor to accountability of data in the cloud, but a supporting factor. This is because in traditional physical server environments housed within companies, the emphasis was on health and feedback on system status and ensuring uptime as server resources are limited and expensive to maintain. In cloud computing, resources like servers and memory are 'elastic', and are no longer limited or expensive . Hence, OS logs, while important, are no longer the top concern of customers. Instead, the customers are more concerned about the integrity, security and management of their data stored in the cloud Systems.

Even though the file system is technically part of the OS, we explicitly include it as a major component in a file-centric system layer. This is because, in order to know, trace and record the exact file life cycles, we often have to track system read/write calls to the file system. From the system read/write calls, we can also extract the files virtual be secure and privacy-aware (to ensure that the logs themselves cannot be tempered with or be a source for knowledge inference); be (eventually) consistent and complete (similar to the ACID properties known from database transaction processing); be transparent/non-invasive; be scalable, e.g. avoid exponential explosion of provenance data through application of summarization techniques be persistent over the long

term; allow for multiple tailored views (to permit access based on While current cloud providers typically support a weaker notion of consistency, i.e., eventual consistency, it is important to have mechanisms to allow for rollback, recovery, replay, backup, and restoring of data. Such functionality is usually enabled by using operational and/or transactional logs, which assist with ensuring atomicity, consistency, and durability properties. Logs have also been proven useful for monitoring of operational anomalies. While these concepts are well established in the database domain, cloud computing characteristics such as eventual consistency, "unlimited" scale, and multi-tenancy pose new challenges. In addition, secure and privacy-aware mechanisms must be devised not only for consistency logs but also for their backups, which are commonly used for media recovery.

WORK FLOW LAYER:

The workflow layer focuses on the audit trails and the audit-related data found in the software services in the cloud. High level fraudulent risks such as procurement approval routes, decision making flows and role management in software services run within the cloud has to be monitored and controlled. In a service oriented architecture , services from several sources are composed to perform higher-level, more complex business functions. The accountability of the services and their providers within the clouds also have to be manage.

Accountability is also required in service oriented architectures in cloud environments. When composing services from existing service components, we also face the problem of trust. With cloud computing, service components can proliferate and their access is virtualized. This makes composition easier and practical. Meanwhile, the source of services may or may not be trustworthy, which presents a major problem in cloud computing. This can be explained using the following example. Let us assume that we are developing a Web portal and we are designing this by integration of the services into a portal. Some of the services may be malicious (for example they manipulate data passing through). Therefore, the portal may or may not be a valid software and perform according to the expected design or according to the contractual agreement. In this scenario, the achievement of accountability of services can help us to investigate such scenarios.

ABUSE AND NEFARIOUS USE OF CLOUD COMPUTING:

This threat is relating to the shortcomings of registration process associated with cloud. Cloud Service Providers offer IAAS and PAAS to their customers with a minimum requirement of a credit card. By taking advantage of this registration process, hackers may be able to conduct susceptible activities like Spamming and Phishing. Initially, PAAS providers have suffered from this attack. However, recent evidence shows that hackers have begun to target IAAS vendors as well (CSA-Cloud Security Alliance).

IN SECURE APPLICATION PROGRAMMING INTERFACES:

Software interfaces or APIs are used by customers to interact with cloud services, which must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them. Cloud providers provide a set of software interfaces or APIs that customers use to manage and interact with the cloud services. The security and availability of cloud services depend upon the security of these

basic APIs [14]. Without proper management of authentication, it leads to Insecure Interfaces. To maintain the secrecy of cloud data, the interfaces must be designed to protect against both accidental and malicious attacks. Malicious insider, working as a cloud employee, collecting confidential data or taking complete control of the cloud services with minimal or no possibility of detection [15]. Therefore it is a important challenge as to how an organization can restrict its internal employees, contractors, vendors and other trusted people who have access to critical resources from within the network.

This key challenge can be addressed to a certain degree by enforcing strict supply chain management and conducting a comprehensive supplier assessment . Authorization plays a important role in securing the cloud. Transparency is very important in the information security and management. When a cloud provider hires their cloud employees, certain factors such as hiring standards, policies regarding how their employees can access to virtual & physical assets and how the employees are being monitored in their work are to be clarified. If the cloud provider does not consider the significance of the above factors, this situation may create more opportunities to the hackers. Top threats for Cloud Computing like Data loss or Data leakage may due to how the data is structured. Firstly, data of an organization must be stored in servers of other nations. This is a significant concern for some organizations. Secondly, the duration of data retained by the Cloud provider, may continue to remain on the provider's servers, even after it has been deleted by the client . Thirdly, improper deletion of data records and alteration of data without proper backup can result in permanent loss of data. Last but not the least, insufficient authentication, authorization and audit control, allows unauthorized parties to gain access into sensitive data. Therefore, Data Integrity must be upheld if CC is to be secured. The businesses' private data are residing on someone else's computer and in someone else's facility which is dangerous. Many things can be wrong with the data such as the Cloud service provider may go out of business. Secondly, the Cloud service provider may decide to hold the data as hostage if there is a dispute.

IV.CONCLUSION

Any application relying upon an emerging technology should consider the different possible threats. Such an application with an inability to anticipate or handle the threats may probably lead to failures. The classification of various security threats/issues presented in this paper would definitely benefit the cloud users to make out proper choice and cloud service providers to handle such threats efficiently.

REFERENCES:

[1] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z; (2010),"Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105, 1-3 Nov. 2010.

[2] Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues, "Towards Trusted Cloud Computing", Conference on Hot Topics in Cloud
Computing 2009, pages 1-5, USA.

[3] Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim, "A Trust Evaluation Model for QoS Guarantee in Cloud Systems",

International Journal of Grid and Distributed Computing, March, 2010.

[5] Zhimin Yang at el, "A Collaborative Trust Model of Firewall-through based on Cloud

Computing", 14th International 0Conference on Computer Supported Cooperative Work in Design, 2010, China

[6] Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE/IFIP International

Conference on Embedded and Ubiquitous Computing, 2010, Australia

[7] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, MateiZaharia. A view of cloud computing.

Communications of the ACM , Volume 53 Issue 4, pages 50-58. April2010.

[8] Siani Pearson. Taking Account of Privacy when Designing Cloud Computing Services. CLOUD '09: Proceedings of the 2009 ICSEWorkshop on Software Engineering Challenges of Cloud Computing, pages 44-52. May 2009

[9] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009

[10] Bansidhar Joshi, A. SanthanaVijayan, Bineet Kumar Joshi,
"Securing Cloud computing Environment against DDoS Attacks",

IEEE, 2011, pp. 1-5.

[11] HaoyongLv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, 2011, pp. 214-216.

[12] AmanBakshi and Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in VM", IEEE, 2010, pp. 260-264.

[13] Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, Shvetank

Verma, Vijay K. Chaurasiya and Rahul Gupta, "An architecture based on proactive model for security in cloud computing", IEEE,
2011, pp. 661-667.

[14] Qinbo Xu, Cuixia Ni, GuangJin, and Xian Liang, "Improve the information security practice Instruction with VM techniques",

IEEE, 2010, pp. 285-288.

[15] AkhilBehl, "Emerging Security Challenges in Cloud computing, an insight to Cloud security challenges and their mitigation", IEEE,
2011, pp. 217-221.

[16] Yoshiaki Hori, Takashi Nishide and Kouichi Sakurai, "Towards Countermeasure of Insider Threat in Network Security", IEEE,
2011, pp. 633-636.

[17] S. Ghemawat, H. Gobioff, and S. Leung, "The Google file system," in Proceedings of the 19th Symposium on Operating SystemsPrinciples (OSDI'2003), 2003, pp. 29–43.

[18] Sara Qaisar, KausarFiaz Khawaja, "Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary

Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329.

[19] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross-Site Scripting Prevention with Dynamic Data
Tainting and Static Analysis", Proceedings of the Network and

Distributed System

[20] Steve Kirsch et al., "The Future of Authentication", 1540-7993/12, IEEE, January-February 2012, pp: 22 – 27.

[21] M. Jensen, "On Technical Security Issues in

Cloud Computing",
IEEE International Conference on Cloud Computing, pp: 109 – 116.

[22] John E. Dunn, "Spammers break Hotmail's CAPTCHA yet again",
Tech-world, Feb. 16, 2009.

[23] Albert B Jeng, Chien Chen Tseng, Der-Feng Tseng, Jiunn-Chin

Wang, "A Study of CAPTCHA and its Application to User Authentication", Proc. Of 2nd Intl. Conference on Computational

Collective Intelligence: Technologies and Applications, 2010.

[24] UdayaTupakula and Vijay Varadharajan, "TVDSEC: Trusted Virtual Domain Security", IEEE, 2011, pp. 57-63.

[25] Shengmei Luo, Zhaoji Lin, Xiaohua Chen, Virtualization security for Cloud computing service", IEEE, 2011, pp. 174-178.

[26] JyotiprakashSahoo, Mohapatra and Lath R, "Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues",
IEEE, 2010, pp. 222-226.

[27] Jenni Susan Reuben, "A Survey on Virtual Machine Security",

Seminar of Network Security, Helsinki University of Technology, 2007.

[28] Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

[29] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing", 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010

[30] HaoyongLv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, 2011, pp. 214-216.

[31] Thomas Ristenpart et al., "Hey, You, Get Off of My Cloud:

Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS09), ACM Press, 2009, pp. 199–212.