Cloud Computing Security Auditing

Irfan Gul, Atiq ur Rehman
Department of Computer Sciences
SZABIST
Islamabad, Pakistan
email: irfan24br@gmail.com, hafizatiq@gmail.com

M Hasan Islam
Department of Computer Sciences
CASE
Islamabad, Pakistan
email: mhasanislam@gmail.com

***Abstract*: In the recent era, cloud computing has evolved as a net centric, service oriented computing model. Consumers purchase computing resources as on-demand basis and get worry free with the underlying technologies used. Cloud computing model is composed of three service models Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) and four deployment models Public, Private, Community and Hybrid. A third party service provider, stores & maintains data, application or infrastructure of Cloud user. Relinquishing the control over data and application poses challenges of security, performance, availability and privacy. Security issues in Cloud computing are most significant among all others. Information Technology (IT) auditing mechanisms and framework in cloud can play an important role in compliance of Cloud IT security policies. In this paper, we focus on cloud security audit mechanisms and models.**

Keywords: IaaS, PaaS, SaaS, TPA, SOA. Cloud security

I. INTRODUCTION

Cloud computing has been envisioned as a next generation information technology (IT) paradigm for provisioning of computing services with a reduced cost and fast accessibility. Big IT giants like Google, Amazon, salesforce.com are providing computing facility like storage, computation and application by pay as per usage through Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) cloud service models. Since cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it is more prone to security threats and vulnerabilities. At present, a major concern in cloud adoption is its security. Intrusion prospects within cloud environment are many and with high gains. Security issues are of more concern to cloud service providers who are actually hosting the services. In most cases, the provider must guarantee that their infrastructure is secure and clients' data and applications are safe by implementing security policies and mechanisms. While the cloud customer must ensure that provider has taken proper security measures to protect their information. In order to ensure, compliance of security policies / mechanisms and to verify whether these policies and procedures are implemented in true letter and spirit, auditing can be employed as a verification tool. Auditing is the process of tracing and logging significant events that could take place during a system run-time. It can be used for analysis, verification and validation of security measures to achieve overall security objectives in a system. Since advantages of cloud computing are obvious, but the security risks associated with each cloud service model hinder its widespread adoption [1]. The externalized aspect of outsourcing makes it difficult to maintain data integrity, privacy, availability and above all compliance check of security measures taken by the service provider. According to a survey in 2009, cloud security was revealed as the top most challenge/ issue of cloud computing among others like availability of services, performance, lack of interoperability standards and so on.

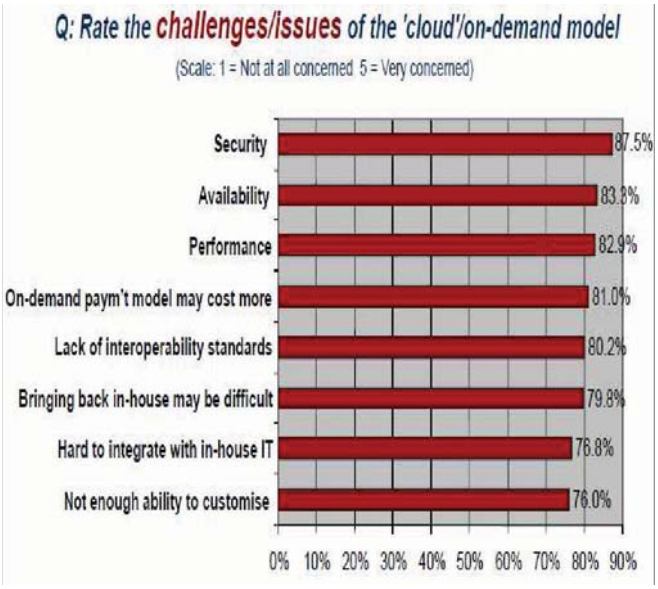

Figure.1- Cloud users' Survey–Security at the top [1]

Over time, organizations tend to relax their security posture and so there is always a need to perform regular security check for compliance of policies through security auditing regularly. Presently, security auditing standards like Statement on Auditing Standards (SAS)-70, ISO/IEC 27001, Health Insurance Portability and Accountability Act (HIPPA) etc. for information security management are available but cloud-specific standard or mechanism is yet to be delivered. In the next section, we'll analyze the related research work in the field of security audit mechanisms and frameworks specifically for cloud environment.

In this paper we have focused on cloud computing security issues and auditing mechanisms. In section I, we've

highlighted security concerns and ranking of challenges/ issues in cloud computing. In Section II, we have carried out the literature review pertaining to cloud security audit. Section III gives a conclusion and section IV gives the idea of future work.

II. LITERATURE REVIEW

A. Data outsourcing in Cloud Computing is fast becoming economically viable for large enterprises. In fact, this data outsourcing is ultimately retrieving user's control over its own data and does not provide any assurance on data integrity and availability. On behalf of cloud user, a third party auditor (TPA) who has resources and experience that a user does not have can be emplaced to audit the integrity of large data storage. But user data privacy is still exposed to a TPA, which is required to be secured against unauthorized leakage. Wang and Sherman *et al.* [2] have proposed a public auditing system of data storage security by developing a privacy preserving auditing protocol. By which auditor can audit without having knowledge of user's data contents. Wang and Sherman also proposed a batch auditing protocol where multiple auditing tasks from different users can be performed simultaneously by a TPA. A public auditing scheme consisting four algorithms (*KeyGen, SigGen, GenProof, VerifyProof*) has been used. *KeyGen* is run by the user to set up the scheme. *SigGen* is used to generate verification metadata. *GenProof* is executed by Cloud Server to provide a proof of data storage correctness. *VerifyProof* is run by TPA to audit the proof from Cloud Server.

The proposed scheme is among the pioneer work to support scalable and efficient public auditing for secure cloud storage. Wang and Sherman *et al.* have presented a privacy preserving auditing protocol by public key based homomorphic linear authenticator (HLA) using random masking technique. A high performance batch auditing protocol is also proposed for TPA to perform auditing tasks for a number of users concurrently and efficiently. However, the authors did not discuss the audit authentication of TPA for a cloud server to respond. Also no details are discussed for authentication handshake between User, Cloud Server or Cloud Service Provider (CSP) and the TPA.

B. Big IT giants such as Google, Yahoo and Microsoft are earning a lot of money by providing storage services like online backups, video hosting and photo sharing to their customers. A customer has to rely on storage service providers to maintain their data integrity. Unluckily, no data storage service is fully reliable as large scale storage systems are complicated and prone to multiple threats that cause data corruption. At present there are no proper mechanisms for policy compliance that leads to protect data by the service providers. In this paper, Shah and Baker *et al.*[3] have proposed some efficient challenge-response auditing protocols by a third party auditor, not only to check data integrity from service provider but also fraudulent customers who claim loss to get paid. Privacy preservation is achieved through zero-knowledge, concealing data contents from the auditor. The suggested protocol has mainly three stages: initialization, audit and extraction. During initialization, user and the service provider enter into an agreement on the stored data object. The auditor confirms both customer & service agree on contents of encrypted data or encryption key, else it would be difficult to resolve future conflicts. In audit stage, auditor can effectively verify the proof of data possession by the service provider through a challenge-response protocol. During extraction phase, the auditor verifies data integrity of data returned to the customer through the auditor. The encrypted data and a "blinded" version of encryption key are forwarded to the auditor. The auditor checks its completeness and passes it to the customer who then recovers the actual data.

The proposed protocols in this paper provide completeness & soundness of data with zero knowledge of data contents to auditor. The protocols divide the data in two parts, an encryption key and encrypted data. The encrypted data rely on a cryptographic hash function and symmetric key encryption. The protocols rely on external authentication methods for communication and do not guard against denial of service attacks. The suggested protocols mostly send small hashes which cause a major overhead for computing HMACs over large data contents.

C. Cloud computing is a new evolving distributed and service oriented computing paradigm. Cloud computing provides services to consumers through Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) models. In a cloud environment, customer's data and applications are placed over remote machines that cause a lot of security hazards. In this scenario, the cloud service providers must adhere to security measures/ policies to mitigate security risks. A strict check on policy compliance must be implemented through IT security auditing. In this paper [4], Chen and Yoon have proposed a framework with master check list for internal and external auditors for reference during auditing. Chen and Yoon have enlisted check lists for Public, Private and Community Cloud deployment models with a focus on IaaS and SaaS service models. IT auditing check list of IaaS model includes: Data location awareness and its legal documentation, data ownership awareness and its verification & destruction process, data protection plan and best practices, data isolation routines checks, User data lock-in and its exit strategy/options, Cloud disaster recovery plan and its frequent tests/updates. SaaS model audit check list comprises of: Data surrender activity and its documented policy, Data format check & availability of readers and monitoring policy for Cloud service availability and performance. Community Cloud check list items are: Community Cloud management and Member exit strategy. Private Cloud check list focuses on reporting control & its compliance, IT architecture & its technical description documentation and disaster recovery & continuity plan.

Chen and Yoon have discussed Cloud IT auditing check lists for IaaS and SaaS to assure a secure cloud computing model. But they have not given any security auditing check list for PaaS service model.

D. Cloud customers can reduce huge investment by hiring expensive IT infrastructure to place their application and data over the cloud. The customer does not have a direct control over its computation and data, similarly the customer does not know the details of the 'service' provided by the service provider. The problem arises when some fault occurs which is not owned by any of the two parties. In this scenario, an accountable cloud is needed to address the issues like data loss, application or infrastructure security, performance and availability. In this paper [5], Andreas has proposed that clouds be made accountable to both customer and provider by using 'audit' as a basic parameter through a third party auditor. To implement audit, a set of basic techniques were discussed which includes tamper-evident logs, that maintain record of past actions performed by cloud customer, provider and user in such a way that a third party auditor can identify the modifications and deletion of entries in the log. The auditor can verify the evidences of faults by obtaining correct records through the logs. Virtualization-based replay can execute virtualized replay of the software over a virtual machine and then record the events for auditing. Trusted time stamping, detects performance faults by adding time information to the tamper-evident logs. Sampling, allows customers to audit checkpoints randomly as various serious problems could have affected most of the segments, though the probability of detection would be high.

The author has described a set of auditing techniques that could be used to make a cloud accountable for correctness and performance. The presented work is among the first to propose cloud accountability for the entire platform. However, they have not proposed a technical solution to address the challenge of data storage security auditing in cloud environment.

E. Data outsourcing in cloud computing is advantageous in terms of worry-free storage management, relief from huge investment and maintenance. It also brings along certain security threats like integrity and availability of outsourced data. Considering the owner's large data and restricted resources capability the responsibility for verification of completeness and availability of data must be delegated to a reliable Third Party Auditor (TPA) without compromising the privacy of data. Cong and Kui et al. [6] have suggested a set of properties for public auditing services focusing cloud data storage security. They have carried out an in depth analysis of publicly auditable data storage security building blocks that constitute: Minimize auditing overhead i.e. the I/O cost for data access and bandwidth cost for data transfer must be reduced. Protect data privacy, in that auditing protocol should not allow TPA to know the data contents when auditing. Support data dynamics, the auditing protocol must be able to support dynamic data updating. Support batch auditing, in which TPA must be able to fulfill concurrent auditing requests from multiple customers efficiently.

The authors have discussed the pros and cons of basic building blocks of publicly auditable secure and dependable cloud data storage. They have focused on the auditing of un-trusted cloud server through a trusted TPA. But they have not discussed the accountability of cloud through auditing, if other cloud entities including owner, user, TPA and service provider as well are malicious and fraudulent.

F. Cloud computing is gaining popularity due to its cost effectiveness in service provisioning. But certain security requirements such as confidentiality, integrity and availability of data are the major security concerns in cloud adoption. Access to cloud by unauthorized users targeting data availability through Distributed Denial of Service (DDOS) attacks is one of the biggest causes of cloud outages. In this paper [7] Sameera and Chan have proposed an identity and access management as a service (IDaaS) model for enterprises using cloud. An organization can completely automate user account provisioning and its auditing by adopting IDaaS model. The main stages of the model consist of: Provisioning and de-provisioning, in that users are provided or deprived of access according to their role in the organization. Authentication and authorization, it involves verification of identity of users or systems and then determining the privileges to be given to legitimate users. Self service, users can change their password, maintain and update their own information. Password management consists of single sign on to access cloud base services and how passwords will be stored in the cloud. Auditing, helps auditors to verify the compliance of different access control policies, periodic auditing and reporting.

Sameera and Chan have discussed two popular identity management protocols Security Assertion Markup Language (SAML) & Open authentication (OAuth) and recommended them to be part of IDaaS model. The proposed model uses multi protocol environment where it has to interface with different cloud service providers' systems. The main drawback of the model is that the enterprise will not be able to know the structure, implementation and services of service provider, also the generated reports of its users may not match the organization's requirement.

G. Cloud computing provides development, delivery and consumption of IT services over a distributed network environment. These services are interdependent on each other and failure of one service can cause unavailability of other service resulting loss of revenue, damaging repute of the enterprise providing services and unreliability over the cloud. To minimize the risks of cloud outages there is a dire need for 'cloud governance' model that could control and manage cloud-based services and storage. In this paper [8], Zhiyun and Meina et al. have proposed a cloud based governance model that securely manages and controls the implementation of cloud services according to recognized policies, service management policies and their audit

procedures. Elements of operational governance model includes: Authentication, i.e. enforcement of identity and access management system. Authorization, it enables implementation of a role-based authorization model. Audit, the collection of information related to the compliance of cloud security and service management policies. Monitoring, the preparation of individual and aggregate data transaction reports, summaries and graphs. Metadata repository, a master repository for service, security and risk management policies of an enterprise.

The proposed governance framework is among the pioneer work that focuses on managing and improving the visibility and trust of cloud services. Though, the authors have not discussed the procedures to implement cloud security and service management policies. Also they have not suggested the need for a third party mediator for compliance and audit of cloud policies.

H. Cloud and Grid computing are the most vulnerable targets for intruders' attacks due to their distributed environment. For such environments, Intrusion Detection System (IDS) can be used to enhance the security measures by a systematic examination of logs, configurations and network traffic. Traditional IDSs are not suitable for cloud environment as network based IDSs (NIDS) cannot detect encrypted node communication, also host base IDSs (HIDS) are not able to find the covert attack traces. Kleber, schulter et al. [9] have proposed an IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect. The architecture of IDS service includes the node, service, event auditor and storage. The node contains resources that are accessed through middleware which defines access-control policies. The service facilitates communication through middleware. The event auditor monitors and captures the network data, also analyzes which rule / policy is broken. The storage holds behavior-based (comparison of recent user actions to usual behavior) and knowledge-based (known trails of previous attacks) databases. The audited data is sent to IDS service core, which analyzes the data and alarm to be an intrusion.

The authors have tested their IDS prototype with the help of simulation and found its performance satisfactory for real-time implementation in a cloud environment. Although they have not discussed the security policies for cloud computing environment and their audit procedures.

I. Public infrastructure cloud provides services to end-users through a multi-tier virtual infrastructure (web, application and database) which is implemented on different abstraction levels i.e. IaaS, PaaS and SaaS. Security risks are the main obstacle in cloud adoption on all levels of abstraction. Faulty network security configurations in public cloud infrastructure can lead to exposure of services to attackers. In this paper [10], Bleikertz and Schunter et al. have proposed algorithms to audit correct network security configurations/policies of a complex multi-tier cloud infrastructure using Amazon's Elastic Compute Cloud (EC2) public infrastructure. In EC2, virtual machines are protected from intruders through a firewall-like feature known as 'security group'. The authors have carried out validation of security assessment of these security groups by two properties. First, reachability i.e. information flow from source to destination allowed by cofiguration and services. Second, vulnerability i.e. attack vulnerability to a service with the help of reachability and attack graphs respectively. The algorithm for auditing the configuration for a reachability policy carries out analysis with respect to reachability graph/set of policies and verifies compliance of its policies. Service vulnerability analysis has been carried out by Dijkstra's shortest path algorithm basing on vulnerability rating i.e. high, medium, low having shortest path with lowest weight. Service vulnerability audit has been carried out by analysis of attack graph against specified policies.

The authors have presented an interesting approach which uses manually obtained reachability and attack graphs for the verification and auditing of network security configurations in public cloud infrastructure. However an automated approach for construction and analysis of these graphs is needed for auditing of such scalable cloud infrastructure.

J. In cloud and grid computing data outsourcing and sharing creates not only security issues like data confidentiality, integrity and privacy but also its access authorization / authentication is of utmost importance. For such distributed environments, a mechanism to protect against unauthorized data access is essentially needed, where even the administrators may not be able to access records without being noticed. Authentication and authorization techniques must be employed to ensure data access attempts and alteration by legitimate users, implementing an effective security policy. To comply with the security policies in distributed environments, data access and modification must be recorded and reconstructed through audit trails. These audit logs can then be evaluated to compile and produce audit reports for violations. In [11], Marco, Feilhauer, Huemer et.al have introduced a new concept of a secure data access architecture, which guarantees data access and modification through a single point of access (SPOA). A secure virtual machine has been modeled to host sensitive data that can be accessed through a portal provided as users interface. All the administrative tasks and users' queries are accomplished through the SPOA, where strict logging is enforced by creating log files to have full control over data access. Auditing of data integrity and access can then be possible by reconstructing and evaluating the audit logs in order to achieve non-repudiation.

Although, this paper covers implementation of a secure data storage access in cloud and grid computing by logging using audit trails through a SPOA. But it does not give out any solution for logs transportation, their interoperability, use of semantics with the log data and their automated evaluation / auditing for complex distributed environments like cloud computing.

K. Cloud and Grid computing support multitenancy and multitasking i.e. multiple customers can perform different tasks through accessing a shared pool of resources over the internet. Distributed nature of these service environments having multiple administrative domains with different security policies and large number of users, creates new security risks. In this case, 'logging' i.e. event recording for examination and reconstruction of sequence of events is one of the solution available for provisioning of audit trails, which can subsequently be used for security audits and forensic analysis. At present, different logging formats are being used that poses the problem of logs correlation and interoperability for creating audit logs and hinders effective security evaluation in complex environment like cloud computing. In this paper [12], Huemer and Tjoa have introduced a secure logging infrastructure based on Extensible Markup Language (XML) technology. The proposed solution aims at automated evaluation and reporting by XML enriched log files using semantics to detect malicious events in a system. For this purpose logging life cycle includes logging configuration (to avoid unwanted information), creation of log files and its protection against modification or unauthorized access, parsing, aggregation, correlation and automatic evaluation to generate automated audit reports.

Although this paper tackles problem of interoperability and incompatibility of log files and their automated evaluation / auditing for distributed and complex systems like cloud & grid computing. But it does not provide a solution to map current log file formats to XML conforming structure that leads to a great effort needed to write parsers for each log file format. Since log files would be maintained by cloud providers in cloud environment, the authors have not addressed the issue of log files tampering and its auditing from user's perspective.

L. Multi-tenancy, data outsourcing and distributed service oriented nature of cloud computing has introduced the issues of security, privacy and data leakage. Risk assessment is considered as an effective approach for evaluating a system for potential risks and maintaining trust among stakeholders. It enables organizations to protect their valuable data / assets through security / privacy assessments and external audits for compliance of policies. Presently, no set standard of risk assessment for evaluating potential security risks and policies compliance mechanism is available for a dynamic cloud environment. In [13], Kaliski and Wayne have presented risk assessment as a service (RaaS) paradigm for measuring and evaluating security risks in cloud computing. The authors have envisioned an automated real-time risk assessment system through which a cloud provider could perform self-assessment or a trusted third party could assess the provider through privileged access and consumers could assess the provider through non privileged access. Also the providers who are consumers of services of other providers could assess them. Automated measurement and analysis is the key for delivering RaaS. Risk assessment service would employ sensors that collect relevant data in real-time environment and an autonomic manager to analyze risks and implement relevant changes. Assessment service would provide an automated service level agreement (SLA) directory or namespace where risk assessment rules and important assets valuation data provided by the users would be entered for continuous assessment in a cloud environment.

Authors have proposed a new concept of 'RaaS' for automated cloud security audit and assessment with its research directions. But they have neither discussed the technical details of the service nor have they practically implemented such a service in a real-time cloud environment.

III. Conclusion

In this paper, we have focused on cloud security issues in general and cloud security auditing in particular. In the literature review section, we have analyzed different cloud security auditing protocols for data integrity and privacy through a trusted TPA. We have also studied data access management architecture using audit trails, a set of auditing techniques to make cloud accountable, an IDS service with a core audit system and auditing frameworks/ models for cloud environments. At the end we have carried out a critical analysis of strengths and weaknesses of these auditing models and techniques. Since cloud computing is in its stage of infancy, a common, interoperable and cloud-specific auditing mechanism need to be designed to maintain trust and transparency within the cloud environment.

IV. Future work

In cloud computing, security auditing can be enforced through a trusted third party auditor or an automated auditing interface / mechanism to improve trust in cloud computing paradigm. Data confidentiality, integrity, authentication and availability are the major security concerns in cloud adoption. In future we intend to develop a tool or service for data integrity auditing that allows auditors to discover and verify true integrity and authenticity without compromising the data privacy. Audit the records available in cloud storage and generate audit reports.

References

[1] Xuan Zhang, Nattapong Wuwong, Hao Li, Xuejie Zhang," Information Security Risk Management Framework for the Cloud Computing Environments", 10th IEEE International Conference on Computer and Information Technology, 29 June, 2010.

[2] Wang, Sherman, Kui, Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", INFOCOM, 2010 Proceedings IEEE, 14-19 March, 2010.

[3] Mehul, Ram, Baker, "Privacy-Preserving Audit and Extraction of Digital Contents", HP Lab Technical Report No. HPL-2008-32, 25 April, 2008.

[4] Zhixiong, John Yoon, “IT Auditing to Assure a Secure Cloud Computing”, IEEE 6th World Congress on Services, 5-10 July, 2010.
[5] Andreas Haeberlen,“A Case for the Accountable Cloud”, ACM SIGOPS Operating Systems Review, 02, April 2010.
[6] Cong and Kui, “Toward Publicly Auditable Secure Cloud Data Storage Services”, IEEE Network Magzine, 19 July, 2010.
[7] Sameera and Chan, “Cloud Computing Security Management”, Second International Conference on Engineering Systems Management and Its Applications (ICESMA), 30 March, 2010.
[8] Zhiyun and Meina, “A Governance Model for Cloud Computing”, International Conference on Management and Service Science (MASS), 24-26 Aug. 2010.
[9] Kleber, schulter, “Intrusion Detection for Grid and Cloud Computing”, IEEE Journal: IT Professional, 19 July 2010.
[10] Bleikertz and Schunter, “Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds”, 17th ACM Conference on Computer and Communications Security, 08 Oct, 2010.
[11] David Huemer, A Min Tjoa,Marco Descher, Thomas Feilhauer, Philip Masser, “Towards a Side Access Free Data Grid Resource by Means of Infrastructure Clouds”, International Conference on Parallel Processing Workshops, 2009. ICPPW '09, 22-25 September, 2009.
[12] David Huemer, A Min Tjoa, “A Stepwise Approach Towards an Interoperable and Flexible Logging Principle for Audit Trails”, Seventh International Conference on Information Technology: New Generations (ITNG), 12-14 April, 2010.
[13] Kaliski and Wayne, “Toward Risk Assessment as a Service in Cloud Environments”, HotCloud'10 Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, 22-25 June, 2010.