Suneeta Mohanty, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 4, April- 2018, pg. 27-32 **ISSN: 2321-8363**
Impact Factor: 5.515

Anomalies Detection Using Public Auditing Scheme In Cloud Computing Environment

Suneeta Mohanty
(School of Computer Engineering/ KIIT Deemed to be University, India)

ABSTRACT: Cloud Computing Environment provides a new way of computing where the cloud users are provided with various services on demand as per their requirements. To get rid of local data storage burden, cloud user stores their data in cloud which gives rise to the problem of security and privacy of stored data. To address the different security challenges of stored data, auditing concept is used in Cloud. Public auditing scheme allows a third party and the user to verify the integrity of remotely stored data. This paper highlighted the anomalies detection using public auditing scheme of Microsoft Azure.
Keywords: Auditing, Public Auditing Scheme, Cloud Service Provider (CSP), Cloud Computing Environment (CCE)

1. Introduction

Cloud Computing Environment provides various computing resources on demand using virtualization technique over the Internet [1]. Cloud users can fulfil their computational requirements using pay per use concept from the Cloud Service Provider[7]. Due to scalability and elasticity properties of CCE, user data are stored in remote areas and taken care by the Cloud Service Provider[8]. User data security became the most sensitive issue in CCE[6]. Public clouds are more vulnerable to various attack than the private cloud. Therefore, to maintain the privacy of the sensitive data and resources, auditing concept was introduced within the Third Party Service Provider for maintaining privacy and integrity of stored data. Public Auditing scheme allow the user along with third party auditor to verify the correctness of remotely stored data.

This paper is organized as follows: In section 2 we have discussed the basics of Auditing in Cloud Computing Environment. Section 3 Public Auditing scheme to detect anomalies. Lastly section 4 concludes our work.

2. Basics of Auditing in Cloud Computing Environment

In Cloud Computing Environment, Auditing is needed in every phases of cloud infrastructure to achieve data confidentiality, privacy, integrity and availability. In the recent scenario, data is being stored, transferred and processed outside the company or organization. Cloud Service Provider (CSP) provides infrastructure elements for metered usage, service level policy and license management, and authentication control [12]. The raw data is not physically controlled by the organization and shared computing environments are also making it public. These kinds of loopholes need more security and privacy. In respect to data access, no controls have been implemented to restrict data modification and no logging events such as access, transmission, modification on data have not been monitored. Limited capabilities for change control and provider feasibility are also the drawbacks of cloud infrastructure. One more thing is that all the physical and logical accesses are managed and maintained by the Cloud Service Provider (CSP). Hence auditing is highly required to maintain the

privacy of the sensitive data, restricted access of computing and physical resources and to check integrity. As the user does not have physical possession of data so the integrity and security of data become the major concern in the cloud computing. Data can get modified by other users or even sometimes cloud service provider for his own benefit can behave unfaithfully towards the users regarding outsourced data. Data integrity means data should be correctly stored on the cloud server without any modification and if any violations i.e. if the data is get lost, altered or compromised can be detected. It must remain in the same state. For example Cloud Service Providers for more space on data centre can discard the user data which has not been or rarely accessed by the user for a longer time or even can hide the data loss incidents to maintain his reputation [14].

Cloud Computing Environment is dependent on the Internet to provide various services to cloud users on demand as a result of which issues like data access control [4] dynamic allocation strategies [5], handling web attacks[3], and controlling sensitive information flow [6]. Auditing for security, Auditing for Risk and Governance, Database Auditing, Auditing for regulation or compliance, Service level agreements (SLAs) Auditing and Third Party Storage Auditing Service Provider are the various aspects of Auditing in CCE[2][10]. In Third Party Storage Auditing Service Provider(TPAS) ,the Cloud user interacts and deploys several applications in cloud[14] and may rely on TPAS to achieve confidentiality, availability and integrity of their stored data. TPAS can verify the integrity of the stored data using Public Auditing scheme[13]. According to Wang et al. [11], auditing can be done without losing the privacy of the user's data.

3. Public Auditing Scheme

Cloud Audit is represented by A6 i.e., Automated Audit, Assertion, Assessment and Assurance API. Auditing can be provided as a service using a common interface that allows cloud provider to automate Audit on their environments and allow authorized cloud user to do likewise via an open, extensible and secure API. Auditing scheme can be provided by the Cloud Service Provider as an API which is very user friendly (Figure1).

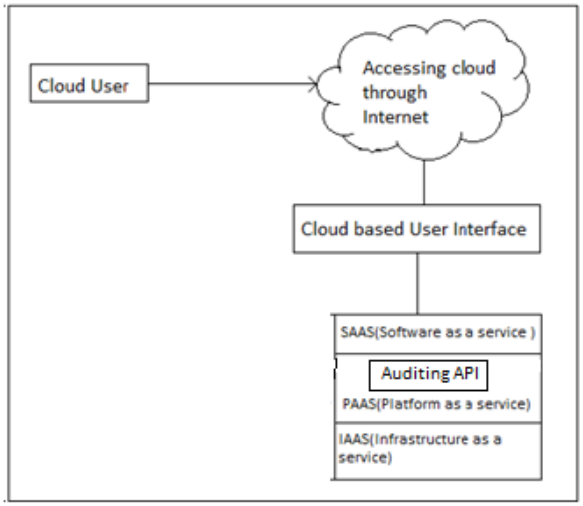

Figure1: Framework showing Auditing API

Taking into account Framework for Auditing in CCE[2], Auditing can be provided as an API, where Cloud user can retain an Audit trail(Fig-2) that help him to streamline activities related to

compliance. Also user come to know about the different activities taking place in the database by whom and when from which he can detect security violations which was not possible earlier.

3.1 How does Auditing track events against Database?

Auditing provides a layer of security for Database, by tracking and logging events and database activity. The audit data can be used to gain insights into database activity, identify potential security concerns and ensure that a record exists for any suspected violations, and to facilitate and streamline compliance-related tasks.

Here we have used Microsoft Azure to show how does Auditing track events against Database. User can configure Auditing for their database using an API on the Azure portal. Once enabled and configured, the Auditing engine tracks all incoming and outgoing events from the designated SQL Database. User can configure categories of Audit logs, and each relevant event is written to the audit log in Azure Storage. User need to select an Azure Storage Account where the audit logs will be saved and specify the set of events that they wish to log Figure2.

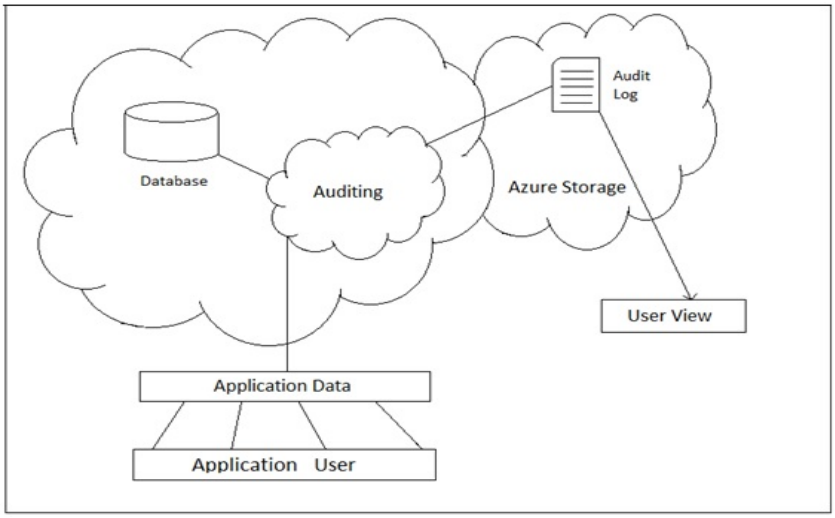

Figure2: Azure storage account

Once Auditing is set up and working, user can view the Auditing dashboard, which provides a quick at-a-glance view of database activity directly from the Azure portal. It displays an updated count of audited database events (freshness up to 15 minutes), that occurred within the past 24 hours. It also shows a breakdown of events by type, so that user can quickly understand the distribution of events occurring on his/her database, and also identify any unusual or unexpected activity.

Both Application user and cloud user can use the built-in reports stored in their Azure storage account to compare activity and trends between databases, and discover anomalies.

Different types of anomalies detected by using Public Auditing Scheme in Azure Database are described as below(figure3):

Number of large data set changes
This Audit log stores the count of Affected Rows value for Data Changes Events often describe the number of rows that were changed in the database. Values which are significantly higher than typical values of user's application may be an anomaly to explore.

Failed Login attempts
This Audit log stores the count of Failed login attempts which indicate unauthorized attempt to gain access to the database.

Total number of rarely used principals(users)
This Audit log stores the information about permission granted to the different users of the database. Users are advised to review permissions rights of the rarely used principal accounts on their database, to prevent unauthorized access.

Total number of suspected event Types
This Audit log stores the count of suspected event type which is rare for user's application. As an example , the template filter Permissions and SqlBatch (SqlBatch classification is used for events which were not classified otherwise)

Total number of operations that took more than 10 Sec
This Audit log stores the count of server duration of different ranges in seconds. High values of server duration may indicate a malfunction in user's application or even a DoS attack on the database.

Total number of operations that returned more that 1000 rows
This Audit log stores the count of Response Rows which is a count of the rows in the response from the database. A value which is significantly larger than the typical values of user's application is an anomaly to observe.

Total number of rarely used client IPs
This Audit log stores the count of rarely used client IPs. As a backend, in many applications the database is accessed mostly from known discrete set of Client IPs. In this case, rarely used IPs are an anomaly to observe.

Total number of rarely used Application Names
This Audit log stores the count of total number of rarely used Application Names. For many applications most traffic to the database is expected from the application. Access from other types of application may be an anomaly to observe.

Once the anomalies are detected Cloud user and Application user can use respective information to address different security challenges. For example ,the "Server Duration" and "Response Rows" fields in the Audit Logs are useful for profiling and debugging. As a backend service Azure Database is expected to be accessed by application stacks, Administrators etc. This interactive report assist with the exploration of the origin of clients that connected to the database and possibly observe undesired access.

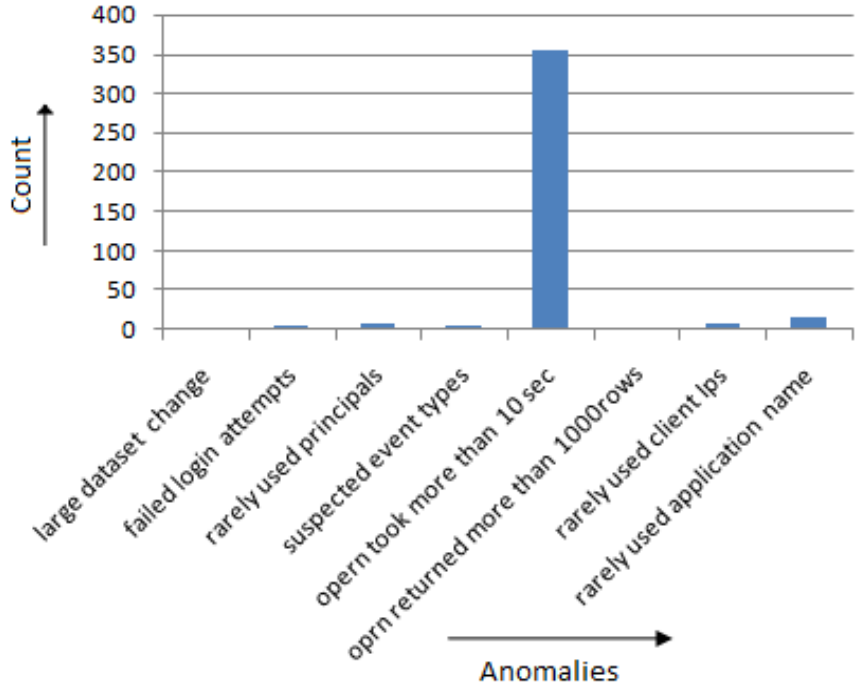

Figure3: Anomalies detected by Auditing

4. CONCLUSION

Cloud Computing Environment provides many benefits to their user but security is major issues in cloud computing. As user store their data to cloud data centers but as user does not know the exact location of their data. So to check the privacy and integrity of data, user can take the help of TPAS. Public Auditing scheme allows both TPA and Cloud user to verify the correctness of remotely stored data. User can use the built-in reports stored in their Cloud storage account to compare activity and trends between databases, and discover anomalies and can take corrective measures to maintain data privacy, integrity and availability.

References

[1] V.Sarathy, P.Narayan, Rao Mikkilineni,"Next generation cloud computing architecture - enabling real-time dynamism for shared distributed physical infrastructure", 19th IEEE International Workshops on Enabling Technologies:Infrastructures for Collaborative Enterprises(WETICE'10), Larissa, Greece,28-30 June 2010,pp. 48-53.

[2] Suneeta Mohanty,P.K.Pattnaik, G.B.Mund "Framework For Auditing In Cloud Computing Environment", Journal Of Theoritical And Applied Information Technology Vol.65,Number 1,July 2014,pp.261-267.

[3] M.Jensen,N.Gruschka,R.Herkenhoner,N.Luttenberger,"SOA and Web Services: New Technologies, New Standards – New Attacks", in 5th European Conf. on Web Services,26-28Nov 2007,pp.35-44.

[4] S. Sundareswaran, A. Squicciarini, D. Lin, S.Huang, "Promoting Distributed Accountability in the Cloud", in 4th IEEE International Conference on Cloud Computing, 2011, pp. 113 -120.
[5] R. Hu, W. Doua, X. Liu, Jianxun Liu," WSRank:A Method for Web Service Ranking in Cloud Environment", in 9th IEEE International Conference Dependable, Autonomic and Secure Computing, 2011,pp. 585 - 592.
[6] W. She, I-L. Yen, B. Thuraisingham, S-Y.Huang, "Rule-Based Run-Time Information Flow Control in Service Cloud", in IEEE International Conference on Web Services,2011,pp. 524 - 531.
[7] Mohanty, S., Pattnaik, P.K. , Mund, G.B.(2017) "Privacy Preserving Auction Based Virtual Machine Instances Allocation Scheme for Cloud Computing Environment", in *International Journal of Electrical and Computer Engineering*, Vol.7(5), pp.2645-2650.
[8] Suneeta Mohanty *et al*, International Journal of Computer Science and Mobile Applications, Vol.6 Issue. 3, March- 2018, pg. 38-43
[9] Wang, Yazhe, Shunan Ma, and Lei Ren. "A Security Framework for Cloud Manufacturing", Volume 1 Materials Micro and Nano Technologies Properties Applications and Systems Sustainable Manufacturing, 2014.
[10] Jonathan Sinclair, "Cloud Auditing", SAP Research.
[11] C. Wang, Q. Wang, K. Ren and W. Lou,"Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010Proceedings IEEE INFOCOM, 14-19 March,California,2010, pp.1-9.
[12] Rajkumar Buyyaa, Chee Shin Yeoa,Srikumar Venugopala, James Broberga, and Ivona Brandicc, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility",Future Generation Computer Systems,Volume25,Issue6, June2009,pp. 599-616.
[13] Rui Xie,Rose Gamble," A Tiered Strategy for Auditing in the Cloud", IEEE International Conference on Cloud Computing,June 2012,pp.945-946.
[14] T. K. Chakraborty, A. Dhami, P. Bansal, and T. Singh, (2013,February), "Enhanced public auditability & secure data storage in cloud computing", in *IEEE 3rd International Advance Computing Conference*, February 2013, pp.101-105.

