A Study on Dimensions of Trust in Cloud Computing

Thasni T
Assistant Professor, Computer Science & Engineering, Presidency University, Bangalore, Karnataka, India

Abstract : ***Cloud computing provides a lot of opportunities to the IT world. Enterprises from startups to large companies view cloud as a good option, because of resource pooling, on demand provisioning and pay as you go model. The most important goal for a cloud service provider is creating a sense of confidence & trust about that cloud provider among service requester. To achieve this, organizations should develop a strategy that is comprehensive , well organized and it should be done with proper checks understanding the future requirements , and by delivering a cloud infrastructure. But, the trust concerns are developing a resistance against the popularity of cloud among the global CXO's. This paper focuses on the various dimensions of trust in cloud computing.***

Index Terms - Cloud, Service Provider, trust ,SLA, Resource Pooling.

I. INTRODUCTION

Cloud computing provides a lot of opportunities to the IT world. Enterprises from startups to large companies view cloud as a good option, because of resource pooling, on demand provisioning and pay as you go model. Through virtualization, cloud can deliver a good number of resources, and these resources can be scaled up or down based on our requirements and can be accessed from anytime anywhere. Cloud brings in efficiency and rapid deployment of services by maintaining transparency regarding underlying infrastructure. But, the trust concerns are developing a resistance against the popularity of cloud among the global CXO's. The security and trust concerns develop the moment the organization data leaves the designated internal firewall and goes into a cloud domain that is public. So, it can be understood that trust management along with information security can be considered as the major challenges in this era of cloud.

There is no clear accepted definition for "Trust in the cloud". Trust management needs to be considered for the cloud service requester and the cloud service provider. For a service provider the most important parameters are - availability ,credibility , security and performance of the service. The different cloud vendors is anticipating that that cloud assets should be secured and to be used by customers who can be trusted upon. The weak connections in the trust chain for instance if the sellers subcontract the work without the client permission or absence of appropriate data on contractual terms can make long lasting ramifications for the customer association. To put it plainly, the trust factor has turned into the most pivotal factor in taking the choice on whether the commitment between the cloud provider and the requester is right.

The critical undertaking for this situation is making trust in the cloud for both the requester and provider .Organizations should start developing a very well comprehensive and well organized cloud strategy which is secured with appropriate checking and balances keeping the future requirements and necessities in mind during allocation of a cloud infrastructure to the customers or receiving a service from the provider. This encourages associations to survey, screen, enhance and upgrade their tasks in the cloud and consequently deal any trust issues efficiently. Its the right time to develop a trusted cloud condition to assist organizations in addressing the customer worries in an efficient way and can change the general worries around cloud into great opportunities. From a customer point of view, the organizations have to include the full scope of dangers that happens in their own environment with third party hosted cloud environments. This strategy will assist them with maintaining a risk exposure that is similar when data and functions are moved from an internal to external premises.

II. DIMENSIONS OF TRUST IN CLOUD ENVIRONMENT

2.1 Access Control

The fields of information security and physical security, the access control means, the selective restriction or control of access to a place or other resource. The end users definitely require different levels of access control, especially from both internal or external data centers through remote access, to perform their tasks or functions associated with various roles and responsibilities. The absence of right security delivering strategies like access control guidelines and policies will lead to unauthorized access and misuse of confidential and sensitive data. So , to handle this situation , a secure ,affordable, always available and easily manageable centralized access control solution is required. So it will allow authorized end users and service providers' in accessing any cloud device or platform securely and efficiently. [1] An effective user revocation model is presented in this paper for mapping is done between revocation requests and defined policies of associated resources. This proposed model has used a revocation engine that is associated or linked with three other stand-alone components to guarantee the security and privacy of affected nodes even after the user revocation requests.

2.2 Trust worthy SLA

Service-level agreement (SLA) is a commitment or agreement between a client and a service provider. The most important aspects of a service - availability, quality, responsibilities – are mutually agreed between the cloud service user and cloud service provider. The most important part of an SLA is that the mentioned services should be provided as per the contact to the customer. This paper focuses on the idea of proposing Trustworthy Service Level Agreements (TSLA) as a means of incorporating security considerations (confidentiality) into a Service Level Agreement (SLA) between a service provider and the customer . In particular, it classifies confidentiality requirements and capabilities according to a typical threat profile for government data classification, by describing five discrete levels of security precautions that can be negotiated between the government and service providers to ensure the confidentiality of sensitive data handled by the providers.

2.3 Secure Data Management

In order to develop trust in the cloud both the service provider and the service requester should have a clear understanding of the data handled ,stored, processed and accessed in the cloud environment. In order to ensure trusted data handling within a cloud environment, all information must be properly classified, segregated and limited access of the information or resources by enforcing policies which grant privileged access to data only on 'need to know basis'. Organizations must give enough focus on data handling, where a customer's requirements around data handling within the cloud are taken care of and also respective regional regulations on how data is stored. Policies should be enforced so as to satisfy the cloud user.

2.4 Accountability

Accountability appears to be a promising approach to the problems mentioned above. Service owner of a cloud which is accountable must be able to detect whether the cloud is functioning as agreed. Ryan K L Ko , Bu Sung Lee, Siani Pearson (2010)[2] mentioned auditability and accountability as important step in increasing trust in a cloud computing environment. To enable an efficient solution to this complex problem, they had proposed a Cloud Accountability Life Cycle (CALC) and three abstraction layers. The term Accountability is replacing to a lot of different meanings within and across disciplines. For instance, the term accountability has been used for a lot of years in computer science to cater to imprecise requirements that are met by auditing and reporting mechanisms. The main context of its use is corporate data governance that is, the management of the usability, availability, integrity and security of the data used, stored, or processed within an organization, and it refers to the process by which a particular goal – the prevention of disproportionate harm to the subjects of PII can be obtained via a combination of public law and regulation, private law such as contracts, self-regulation. Public Law, rules and regulations and premised upon command and control over the regulatory strategies has influenced various national and international privacy protection approaches. But, the effectiveness of regulatory and legislative mechanisms have declined as various technological developments make the underlying regulatory techniques out of use. Accountability enables users develop trust. When it is not obvious to an individual why their protected private data is requested for or how and by whom it will be consumed, this absence of control will lead to distrust and doubt. Besides these, there are also security-related issues and worries about whether the information in the cloud will be secured enough.

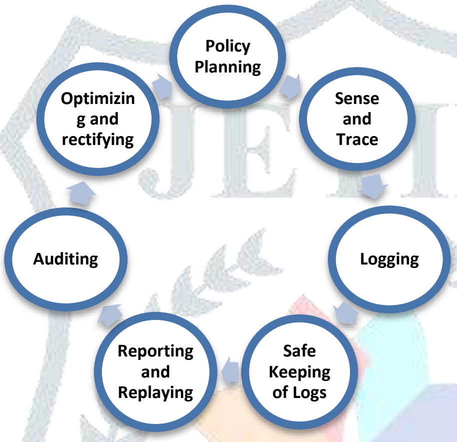

Fig 2.1: The Cloud Accountability Life Cycle

2.4.1. Policy Planning

In the beginning, 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 the observation, there are generally four important groups of data that must be logged: (1) Event data – a sequence of activities and relevant information, (2) Actor Data – the person or computer component (e.g. worm) which trigger the event, (3) Timestamp Data – the time and date the event took place, and (4) Location Data – both virtual and physical (network, memory, etc.) server addresses at which the event took place.

2.4.2 Sense and Trace

The aim of this phase is to start triggering the logging activity whenever an expected event occurs in the CSP's cloud. .Accountability methods and tools should be able to track from the lowest-level system read or 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.

2.4.3 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.

2.4.4 Safe-keeping of Logs

After logging is done, it needs to protect the integrity of the logs prevent unauthorized access and ensure that they are tamper-free. Encryption may be applied to protect the logs.

2.4.5 Reporting and Replaying

Reporting tools generate from logs file-centric summaries and reports of the audit trails, access history of files and the life cycle of files in the cloud. Suspected irregularities are also flagged to the end-user.

2.4.6 Auditing

Logs and reports are checked and potential fraud-causing loopholes highlighted. The checking can be performed by auditors or stakeholders. If automated, the process of auditing will become 'enforcement'.

2.4.7 Optimizing and Rectifying

In this part, security loopholes and problem areas in the cloud are rectified or removed and governance and control of the cloud processes are enhanced.

[4] Proposes a framework based on decentralized accountability to build trust and confidence in consumers. The service owner first authenticates itself to the CSP by providing username and password. If he is already subscribed to that CSP, then access is granted. After entering the system he creates executable JAR file containing encrypted data. In the proposed system, image files are used as sensitive data. Images are added to the JAR file after encryption at the provider side. Compilation is done after adding all the files such as encryption file, files that perform logging, files for handling the data etc. Then JAR is created with the class files and the encrypted image. The checksum of the JAR file is sent to the auditor. Then the executable JAR file is sent to the cloud. Service provider can also check the trustworthiness of the cloud server using automatic JAR checking. In automatic JAR checking, consumer simulation program is used. The authorized consumers are allowed to access the JAR files. The consumer can search for a particular file using a specific keyword. The consumer can download the files from the cloud. The auditor conducts the auditing of files. This audit record consists of the date, start time, end time etc. Integrity checking is done before giving access to the JAR to the consumer. It is done by the auditor. Permission of the consumer is checked before giving access to the JAR by communicating with the cloud server during JAR execution. The encrypted log records are sent to the auditor during access of the JAR file. Service owner can retrieve the log records based on his needs.

2.5 Trustworthy Infrastructure

If the virtualization technology or the third party data center technologies are not secure enough to store and handle customer data, it will impact the trust factor. On a technology point of view, cloud service providers should maintain compliance with proper technical controls, industry certifications and fool proof virtualization technologies for the customers. They should monitor vulnerabilities and provide audit reports at regular intervals.

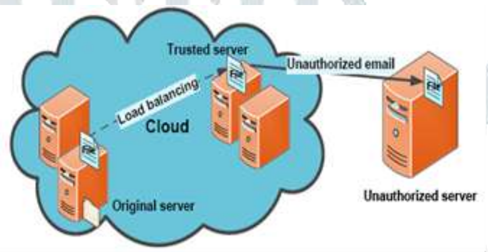

Fig 2.2: A Scenario in Cloud Computing

There exists the fear that administrators and other personnel working for the cloud provider can access our machines and data within, which is a business risk we are taking. Due to this, the major providers of cloud provides its customers an option to manage their own encryption keys, which means that no-one inside the provider can get access even if they tried to. Very few companies are nowadays adopting an approach called as the "hybrid" approach - allowing their more sensitive & secretive data in the private cloud and other data and related applications in the public cloud.

2.6 Legal, statutory and regulatory compliance

Here, compliance means conformation to a rule, such as a policy, standard, specification or law. In Regulatory compliance, organizations strive to take steps to comply with relevant laws, polices, and regulations. It is highly critical to meet the audit and compliance standards in the cloud environment. Cloud customers must adopt the service after analyzing the history of the service providers in terms of security policies. To ensure trust, the service providers must adhere and comply with the cloud and data security regulations pertaining to a country.

They should administer third party audits with regular reviews and assessments to identify whether there are any issues in the established policies or contractual terms. They should document and keep reviewing and updating the legal, statutory and regulatory compliance as well.

2.7 Transparency

The cloud computing vendors should be more transparent in their security policies and practices to become a trusted and secure partner to enterprises in such an environment. Beyond attesting to their security controls the vendors they also need to prove it. Large organizations, when compared to their smaller and medium-sized counterparts, are in an advantageous position to demand such kind of transparency from cloud vendors. But cloud service providers would be well served by offering such transparency to all prospective customers. Greater transparency could become a competitive differentiator for cloud vendors, because so many organizations is viewing security as critical to their cloud adoption.

I. Conclusion

The significant task is creating trust and confidence in the cloud for both the cloud service provider and service requester. Despite all the concerns regarding privacy, security and trust, Cloud model will continue to evolve in the coming years. Organizations have to adapt and improve ways to protect the information stored in the cloud and keep building trust around this disruptive business model.

II. Acknowledgement

I thank everyone who provided insight and expertise that greatly assisted me in doing this research.

References

[1] Maël Kimmerlin, Peer Hasselmeyer, Andreas Ripke, “An effective user revocation for policy-based access control schema in clouds,” Cloud Networking (CloudNet), 2017 IEEE 6th International Conference, 2017.

[2] Ryan K. L. Ko, Bu Sung Lee, Siani Pearson, "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," Springer Advances in Computing and Communications in Computer and Information Science, Volume 193, pp 432-444, 2011.

[3] Yudhistira Nugraha ; Andrew Martin, " Towards the Classification of Confidentiality Capabilities in Trustworthy Service Level Agreements ," Cloud Engineering (IC2E), 2017 IEEE International Conference 2017

[4] Thasni T,P Mohamed Shameem," A Framework Assuring Decentralised Accountability in Cloud",International Journal of Research in engineering and Technology,Volume 3,07,2014

[5] Siani Pearson, "Toward Accountability in the Cloud," View from the Cloud, IEEE Internet Computing, IEEE Computer Society, July/August issue, vol. 15, no. 4, pp. 64-69, 2011.

[6] Marianthi Theoharidou, Nick Papanikolaou, Siani Pearson and DimitrisGritzalis, "Privacy Risk, Security, Accountability in Cloud Platforms," IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 177 – 184, 2013.

[7] Marco Casassa Mont, Siani Pearson and Pete Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," Proc. Int'l Workshop Database and Expert Systems Applications (DEXA), pp. 377-382, 2013.

[8] Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transaction on dependable a secure computing, VOL. 9, NO. 4, pg 556-568, 2012.

[9] Cong Wang, S. M. Chow, Qian Wang, KuiRen, Wenjing Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transaction on Computers, 2013.

[10] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2011. Ramasundram, S.P.Victor, "Text Categorization by Backpropagation Network," International Journal of Computer Applications, vol. 8, no. 6, 2010.

[11] Mahender, Vandana Korde C Namrata, "Text Classification and Classifiers: A Survey," International Journal of Artificial Intelligence & Applications, vol. 3, no. 2, 2012. S.K. Dhurandher, S. Misra, M.S. Obaidat, V. Basal, P. Singh and V. Punia,'An Energy-Efficient On Demand Routing algorithm for Mobile Ad-Hoc Networks', 15 th International conference on Electronics, Circuits and Systems, pp. 958-9618, 2008.