Review On Privacy And Compliance Issues In Cloud Computing

K Harish Kumar
Asst.Professor, Dept of Computer Science
Mahatma Ghandhi University NALGONDA,TELANGANA, INDIA.

Abstract- *Cloud computing became more prominent technology since past few years. Migrating to cloud reduces the hardships of maintain infrastructure and administration. Most of the business enterprises are transforming their core businesses to cloud computing because its features like scalability, agility, cost-effectiveness, and one can access the data in the cloud from any location. However there are certain security, privacy and compliance issues to be considered while adapting cloud services. Cloud service providers (CSPs) must fulfill privacy, security and compliance standards in order to safeguard client's data over the cloud. In Clients are forced to rely on Service Providers for security for their data on cloud. Initially cloud service providers are not much concerned about the security, but with increase in its adaptability and competition among, now they are focusing on safety and privacy of client's data with appropriate compliance regulations and industry standards. HIPAA, FISMA, GLBA, PCIDSS, and SOX etc. are some examples for compliance regulations. Good Compliance regulations drive the success of business in cloud industry. Maintenance of data privacy and compliance is big issue for Cloud providers. Objective this paper is to give the brief review of privacy and compliance issues involved while migrating to cloud computing. The data used in this paper is secondary data obtained from various sources like journals, white papers, websites, and blog articles.*

Keywords- Cloud Computing, Cloud Service Provider, Compliance, Privacy, Data Security.

I. INTRODUCTION

Cloud computing is transforms the computation process from local computers to cloud providers over the internet. Cloud computing renders storage and computing services through internet. These services are accessed on pay per serve basis. There are three types of services are provided by Cloud Service Provides (CSPs) to clients. One is SaaS (Software as a Service), second service is PaaS (Platform as a Service), and last one is IaaS (Infrastructure as a Service) [1, 2]. Clients can access software applications in SaaS, in IaaS It Infrastructural services like processor and storage space etc. are provided to clients. PaaS offers computing platforms to clients so that they can develop their own applications. Cloud also serves four deployment models public, private, community and hybrid model. Cloud services are made available to normal people in public cloud deployment model, in Private deployment cloud services are provided for particular company, in community model services are provided for specific communities, and hybrid cloud is a combination of public and private deployment models. The significant advantage of cloud is that it reduces the cost, preservation and administration hardships of IT infrastructure and services for clients. Cloud client can access its services from anywhere [2-5]. Notwithstanding its applications providing security for cloud user's data became major hindrance for its adaptation. Clients are not familiar to the location and privacy of their data. Compliance, data privacy, reliability, trust and security are crucial motives that are keeping majority of customers out of this business [6]. When client organizations migrates its operations to cloud environment they lost control of their applications and other sensitive data. This means client organizations must have rely on CSPs for security and privacy of their data. So they must have some legible regulations before adapting cloud services. At the same time CSPs must come up with security policies that can gain client's trust and safeguards client's data. These policies must be in compliant with client. Privacy and compliance issues must be taken into consideration before deployment. Organizations must pay attention to the data safety and privacy measures and policies of Cloud Service Provider, and must know that they are in compliant with requirements of the organization [9]. Data privacy protection is crucial and foremost objective of cloud computing security. It is difficult task in cloud computing since cloud shared environment which relies on shared infrastructures. So there is a danger that sensitive data can be vulnerable to intruders. Safeguarding of client's privacy is the substantial challenge for Cloud Service Provides.

Compliance maintenance is another big issue for the success of cloud. When data is transferring between different geographical locations it is important to maintain compliancy regulations according national and international regulations. Cloud Service Provides must ensure transparency of data access to cloud customers, with confidentiality from otherworld by following compliance regulation. This is most complex task for CSPS. Ultimately there should be some policies between CSPs and costumers to win the trust of cloud customer [10]. These policies should provide data privacy and better compliancy management between cloud provider and customer. While adapting these policies CSPs must focus on so many privacy and compliance issues such as lack of transparency and control over client's data, data exposure over the cloud, illegitimate access of sensitive information, data integrity, vast escalation of data and maintaining legal regulations etc.. This paper reviews those issues to overcome for the successful outcome of cloud business.

II. PRIVACY ISSUES IN CLOUD COMPUTING

Data security, privacy and ensuring data confidentiality is became stressful task considering with outstanding progression of cloud computing. The reason for this is shared characteristic of cloud computing. Customers lost control and confidentiality of their data when they move their data to cloud, this indicates that the cloud computing paradigm not suitable when confidentiality matters for some organizations who eventually likes to keep their services and data private [7]. Most of the business enterprises manifesting their un-likeliness towards cloud computing because they don't want to keep their data and applications outside of their own data centers. And moreover there has been a problem of sensitive data exposure to outside world that creates legal and administrative problems of the data being stored or migrated. When service provider compromises or when user's data is accessed by unauthorized persons data confidentiality issues arises. This happens because service providers doesn't intimate about their security mechanism drawbacks which leads to user data leakages or when service providers share user's data with others in absence of user's authorization. So it is difficult task to maintain data privacy in cloud computing with sharing of resources [10]. Some those privacy issues discussed below.

A. Lack of control

Lack of control is a significant issue to look after in cloud computing as user based control is not possible. Most of security blackouts and data breaches are happening because of this issue. For example if cloud customer opts for SaaS service provider takes control of data storage and maintenance with customer is provided limited control and visibility. Customers are unaware about service provider's security mechanisms, employee details and their skills of expertise. Thus, there should be some legal regulations followed by service provider so that those regulations serves the needs of cloud customers and gain the trust of cloud customers. Since customer's data managed in the cloud on which they lack control there is possibility of several incidents like data theft, or unauthorized access of data may happen. Moreover there is no clarity about customers can access all their data placed on cloud or deletion of data in comply with customer's request. Also there may be chance where employees mistakenly send sensitive data to unintended user.

B. Unauthorized Data Access

Most of the cloud service providers utilize customer's data for their secondary business purposes, without the knowledge of customer, which may fetch income for service providers. This is big risk factor with cloud computing. Once you put your data on cloud, you were unaware about unauthorized access of your data.

C. Data Outages

Most of the cloud service providers utilize customer's data for their secondary business purposes, without the knowledge of customer, which may fetch income for service providers. This is big risk factor with cloud computing. Once you put your data on cloud, you were lost control of your data and service provider solely responsible for safety of your data. Cloud storage services may experience failure for the applications hosted or may face permanent breakdown of services may occur at service providers services. These events cause temporary or permanent data outages.

D. Data Provisioning

Data provisioning is another issue to consider with dynamic nature of cloud computing. Sometimes data in cloud becomes outdated with dynamic provision of data. And also sometimes it is on clear that who is handling the issue of ensuring judicial needs for client's personal data. Further it may not determined that the role and trustworthiness of cloud subcontractors who involves in processing and their authority over data.

III. COMPLIANCE ISSUES IN CLOUD COMPUTING

Service providers must ensure the responsibility of compliance requirements, and at the same time cloud clients must describe and determine their requirements to be compliant with. Accordingly most of the enterprises face difficulties in situations. Clients should have to estimate compliance with regulatory requirements throughout the cloud access, data encryptions, data storage, and other regulations. Compliance is a substantial problem, or challenge for cloud service providers as well as clients whenever they put their sensitive data on cloud. Clients need to ask service providers about How compliant are service providers with government and industry regulations, about recovery and storage mechanisms of their data, about safety of their sensitive data and about cross border regulations [18]. Eventually, clients need to trust the cloud service providers and service providers must ensure transparency for clients. But however it is somewhat difficult to maintain confidentiality while providing transparency. Service providers must let clients know about rate of risk while moving to cloud. The risk rate will differs according to the confidentiality of the data that is processed on cloud and the level of regulatory faults to which the organization is unprotected. Below are some compliance issues to consider for the cloud business.

A. Transparency Issues

Service providers must give assurance for the safety, confidentiality, availability, integrity and accountability of client's sensitive data. Absence of transparency and providing less over client's data is an issue in public cloud environment. In public cloud the clients' data may be replicated over different countries and regions this raises issue of data not comply with privacy regulations in other countries [18]. It is a big issue to maintain transparency and confidentiality.

B. Complexity Issues

Usually compliancy regulations are inscribed by lawyers and they are of extensive length. So it is difficult for people read and understand such lengthy information. Furthermore there may be some inconsistent, unwanted and unreliable regulations.

C. Overlapping of regulations

Sometimes it is essential for service providers to keep up multiple regulations in order to carry out clients' requirements. This may cause high maintenance and implementation costs, inconsistencies and duplication of efforts. These overlaps can only be identified at architecture level [18].

D. Data Transportation Issues

Data transfer between different legal jurisdictions puts your data at risk and raises Governance, accountability legal complexities. In cloud business wrong business partners are difficult to deal with and difficult asses. With jurisdiction issues, it is difficult to decide which law is applicable and which legal solution can be applied. Perceiving essential compliance requirements is difficult in these situations. There also a chance of violating local regulations while transferring data between different countries.

E. Security Issues

Cloud services required to deal with different kinds of security attacks. With the shared nature of cloud computing overall compliance will be affected. In most of the cases compliancy needs to deal with security of cloud. Since clients upload their data on cloud they have look at all the security aspects of service provider. There should be service-level agreements (SLAs) for conducting security audits of service provider's compliance. Service providers are need to win the customer's trust by maintaining strong and potential security handling mechanisms. Notwithstanding, different groups who doesn't have full compliance is often handled by different groups who don't have enough skills handles the compliance.

IV. CONCLUSION

Security is the critical facet to consider with dynamic continuous expansion of cloud. Data on cloud must follow the compliance regulations and guidelines. But it is difficult and there are some issues while maintaining the compliance. This successfully reviewed those issues which may be overcome for the success the business. Compliance maintenance is significantly useful for cloud business organizations from deferent point of views such as it allows business to follow the legal rules and helps us to get rid of jurisdictional penalties, increases the company's brand value, Avoids Financial Damages, maintenance of audit records as per law. For the success clients need to trust their service providers at the same time service provider must let know clients about security and storage mechanisms and data on cloud must be stored in an encrypted format to gain the client's trust. At present most of the service providers are realizing the importance of compliance and providing compliancy services directly to achieve compliance.

REFERENCES

[1] A. Yousif, M. Farouk, and M. B. Bashir, "A Cloud Based Framework for Platform as a Service," in Cloud Computing (ICCC), 2015 International Conference on, 2015, pp. 1-5.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[3] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," Communications Surveys & Tutorials, IEEE, vol. 15, pp. 843-859, 2013.

[4] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional

evolution", Telecommunications Policy, vol. 37, 2013.

[5] W. Jansen and T. Grance, "Guidelines on security and privacy in public cloud computing," NIST special publication, vol. 800, pp. 10-11, 2011.

[6] Shweta Khara, Prof. Ankita Gupta, "Security Issues in Cloud", IJIACS, Volume 6, Issue 1, January 2017.

[7] Ramakrishnan Krishnan, "Security and Privacy In Cloud Computing", Western Michigan University, Spring 2017.

[8] Sokratis K. Katsikas, "SEPRICC: Security and Privacy in Cloud Computing",The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization, Athens, Greece, February 2017.

[9] Sherin Sreedharan, "Security and Privacy Issues of Cloud Computing; Solutions and Secure Framework", IOSR-JCE, Volume 10, Issue 4, Mar - Apr 2013.

[10] G.Praveen Kumar, S.Kavitha, "A Survey on Security and Privacy Issues In Cloud Computing", Vol. 5, Issue 7, July 2017.

[11] Siani Pearson and Azzedine Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", 2nd IEEE International Conference on Cloud Computing Technology and Science, Cloud and Security Research Lab, HP Labs, Bristol, UK.

[12] Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", ijacsa, Vol. 7, No. 4, 2016.

[13] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu, "Review Article Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks, 2014.

[14] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", NIST.

[15] Usman Ahmad Usmani, Shah Shoib Faizan and Mavera Usmani, "Security and Privacy issues in Cloud Computing and Providing Platform for E-learning", IJICT, Volume 4, Number 5, 2014.

[16] Dereje Yimam, Eduardo B. Fernandez, "A survey of compliance issues in cloud computing", Journal of Internet Services and Applications, 2016.

[17] "Achieving compliance in the cloud", www.cso.com.

[18] https://www.datamation.com/cloud-computing/governance-and-compliance.html.

[19] https://social.technet.microsoft.com/wiki/contents/articles/3800.compliance-issues-in-the-cloud.aspx.

[20] https://www.druva.com/blog/maintain-security-compliance-cloud.

[21] https://www.infoworld.com/article/3162737/compliance/managing-compliance-is-easier-in-the-cloud.html.

[22] https://www.tripwire.com/state-of-security/regulatory-compliance/regulatory-compliance-cloud.

[23] http://www.hexatier.com/it-compliance-as-a-service-caas-is-it-right-for-you.

[24] https://www.cio.com/article/2901034/cloud-computing/your-guide-to-compliance-in-the-cloud.

[25] Cloud Security and Compliance: A Primer, SANS Institute Reading Room.

[26] Soha Alboghdady, Stefan Winter, Ahmed Taha, Heng Zhang, Neeraj Suri, "C'MON: Monitoring the Compliance of Cloud Services to Contracted Properties", ARES '17, August 29-September 01, 2017.

[27] "Critical Security and Compliance Considerations for Hybrid Cloud Deployments", 451 ADVISORS, July 2016.

[28] "Understanding Compliance in the Cloud", www.evolveip.net.

[29] "COMPLIANCE IN THE CLOUD: Continuous Management & Reporting", evident.io.

[30] J. Nicholas Hoover", Compliance in the Ether: Cloud Computing, Data Security and Business Regulation", Volume 8, Issue 1, 2013.