Progressing the Security Landscape of Cloud by Incorporating Security Service Level Agreement (Sec-SLA)

Joydeep Choudhury, Indushree Banerjee, Amitava Nag and Indika Parera

Abstract Gathering personal information of individuals', in return to provide different personalized services, continues to grow. The adaptability and flexibility of cloud that allows mobility of data access and multiple ownerships provide a favorable platform for users and service providers to adapt Cloud services for storing and accessing personal data. However data flow from one level to another service level of cloud may cause data loss or leakage and put the privacy of individuals at risk without them being aware of it. Ensuring privacy of information on Cloud, presents a major challenge to be tackled by future researchers. This paper aims at providing an overall picture of cloud privacy and security at its different level of architecture and discusses the proposed solutions. It will further provide detailed analyses of the various adopted techniques. We will also discuss Security-SLA as a security protection mechanism for cloud users. Further we will try to highlight the areas which can be further researched and make cloud a more secure place to store data.

Keywords Cloud computing · Service level agreement · Security · Privacy · Identity management

Joydeep Choudhury · Indushree Banerjee · Amitava Nag (✉)
Department of Computer Science, Academy of Technology,
Aedconagar, Hooghly 712121, West Bengal, India
e-mail: amitavanag.09@gmail.com

Joydeep Choudhury
e-mail: joydeepchoudhury193@gmail.com

Indushree Banerjee
e-mail: banerjee.indushree@gmail.com

Indika Parera
Department of Computer Science, University of Moratuwa,
Katubedda 10400, Moratuwa, Sri Lanka
e-mail: indika@cse.mrt.ac.lk

J.K. Mandal et al. (eds.), *Proceedings of the First International Conference on Intelligent Computing and Communication*, Advances in Intelligent Systems and Computing 458, DOI 10.1007/978-981-10-2035-3_7

1 Introduction

Cloud has become an important and growing technology which generates revenue options in both industries as well as in academics, but it is still in the process of evolving and considered an enigma when security and privacy comes into perspective. The term "Cloud" was coined by the telecommunication industry when the providers started to use Virtual Private Network or VPN service data communication [1]. At present cloud services promotes itself as an encouraging technology to deliver infrastructure and resource to its users as pay-as-you-go style and by reducing the cost of IT infrastructure for new and small business [2]. Users in general are provided access to a web based interface for connecting and storing their personal data without being aware of the storage location or resources they are using during the operation of a certain application. Storing their personal data in an unknown location with other consumers can possess several threat especially when unknowingly data could rest on the same resources of a competitor's private information application [3], thus a constant drawback of getting data manhandled and misused becomes a nightmare for many organizations and users concerned about their privacy. Apart from improper access and deletion of data from cloud storage there is a significant privacy issue that makes users rethink about the adaptation of cloud [4] which is losing complete ownership. In spite being clearly predefined in various agreements there is no surety that redundant data have been completely discarded once the partnership or employability of a certain vendor is terminated. Various attempts have been made in past to safeguard privacy of individuals and agencies by utilizing different access control mechanisms and security agreements within cloud, but still it is not clear how provider deals with data and if at all the provider maintains integrity and authentication.

With this paper we try to highlight the major challenges faced by users and organizations acquiring Cloud services in general. Introduction gives an overview of the various topics being covered by the paper. Section 2 provides an in depth discussion of the Cloud architecture being currently implemented by the service providers. Section 3 delves deeper into the limitations and security threats specifically presented by Cloud infrastructures in its different layers. Section 4 will discuss a detailed analysis of the protection methods currently used. Section 5 deals with the Service Level agreement and explains the necessity and utility of SLA with respect to safeguarding users from being victimized. Section 6 introduces the concept of security SLA. Finally the last section provides future direction and concludes the paper.

2 Cloud Architecture

The vital characteristic of cloud that makes it a success are noted as on-demand, pay-as you-go, self-service, ubiquitous network access, which allows geographic area independence, resource pooling and rapid elasticity [5] making it adoptable to small businesses. Privacy and security issues of cloud are inbuilt issues, and in order to completely understand the subatomic reasons for these issues it becomes mandatory to revise the architecture of Cloud. Cloud is divided into four layers in a top down order i.e. application, platform, infrastructure and hardware. These are again grouped together into three layers in accordance to the service oriented business model i.e. Software as a Service (SaaS), Platform as a Service (Paas) and Infrastructure as a Service (Iaas) [6]. Figure 1 illustrates structure of cloud with all layers and an overall utility of each layer. Application layer is the topmost layer of cloud architecture which delivers software that a user need. In business model it is called Software-as-a-Service. It provides networked based access and management of commercially available software from a centralized location to the users [1]. Google App is an example of mostly used SaaS.

Second layer is on the top of infrastructure layer and is mainly responsible for providing all computational resources like programming framework and operating systems. This is called Platform-as-a-Service. Main aim of this level is to reduce the load of direct deployment of application in VMs. Google App engine is an example of PaaS as it provides API support to users for executing storage, database for an

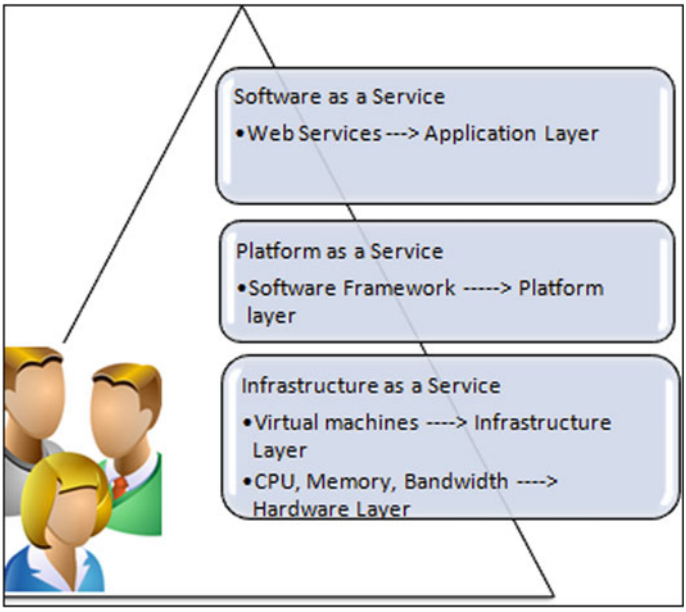

Fig. 1 Cloud structure

application. Infrastructure and Hardware layers are the layers that are responsible managing physical and virtual resources of the cloud. Hardware layer is consists of servers, switches, router and storage units. Data centers are example of hardware layer of cloud. Infrastructure layer is also called virtualization layer as it creates virtual pool of resources. In this level VM technologies, such as Xen, KVM, and VMware etc., are used to partition the physical resources [6].

3 Cloud Security Issues in Different Layers

Cloud is a combination of numerous well established technologies which include grid and distributed computing. Internet is used as a delivery medium to provide services to its users [7]. When the user progress from IaaS to PaaS to SaaS more abstraction of technology is introduced and because of this stored data in cloud are not in direct control of the user and these data are transmitted using Internet makes the user's privacy and security at of higher risk. Whenever a user starts to avail a service, different service level of cloud infrastructure take part in the process and the corresponding privacy mechanisms play a crucial role in the process [2].

3.1 Identity Management

In order to provide location independent data the cloud providers rely on redundant data storage and uses personal information of individual user in the storage to authenticate, and because of this it has to assure the protection of their data inside cloud servers [8]. User privacy can also be compromised while using the communication channel to query the cloud for some information. For example if a user send a query to the cloud regarding a cancer medicine, then an observer of the communication channel can infer that the user or someone related to the user might have cancer disease. There must be some privacy protection mechanism to protect user form this type of risk [9] (Table 1).

Table 1 Security challenges in different layers of cloud

Layers	Issues on that layer
SaaS	Identity management
	Virtualization vulnerability
	Authentication and authorisation
	Data integrity
	Availability
PaaS	Application security
IaaS	Hypervisor attack
	DDoS attack

3.2 Multi Tenancy and VM

Multi tenancy is an essential property of cloud. It helps Cloud Service Providers (CSP) to share resources to different user and make computation very efficient and highly scalable. The main security concern of user is that their personal data might be exposed to the third party as they all are using the same computational space in the cloud. In the virtualized environment where one physical machine hosts multiple users; there is always an associated risk that the other user can monitor its neighbor's activity and lead the other users of the VM accessible to it.

3.3 Attack on Hypervisor

Hypervisor is an application or a computer that creates and run virtual machines to provide the resources to its users. Most common types of attacks are Virtual library checker, encryption attack and migration attack [10]. In migration attack and encryption attack the attacker use the network and virtual machine software vulnerabilities to gain access to the data.

3.4 Availability

Availability means cloud providers must ensure that the service is always available to the authorized user even if a security breach is detected [11]. DDoS attacks makes the services and data unavailable to the user and this makes a real threat for cloud users.

3.5 Lower Layer Issues

The lowest layer of the cloud is hardware layer which is mainly consists of physical machines. A large number of attacks are done in this layer and causes data loss. Most common attack on this layer is Distributed Denial of Service (DDoS) or Denial of Service (DoS) attack. The attacker sends multiple requests to the server in a very short period of time. This technique is called "flooding". With this the server become busy to process unwanted request and thus occupy the bandwidth of the network. Which in due course disrupt service of an authenticate user and prevent access to a service [12]. Cookies poisoning is another type of attack in this physical layer where the attacker modified the cookies into gain access to the cloud.

4 Protection Methods

There are ample amount of work has been done to protect user data from the above attacks, but traditional security issues are still present in cloud environment. In this section we will describe some of solutions of privacy and security issues proposed by researchers. Roy et al. [13] introduced Ariavat, a privacy protection on Map Reduce Systems. This system was built using a combination of mandatory access control and differential privacy technique. The main functionality of the proposed system was to provide end-to-end confidentiality along with integrity and privacy in cloud infrastructure.

IBM, in 2009, introduced a homomorphic encryption scheme to protect data privacy [14]. In this method a user stores it data in an encrypted format in some unknown server, and when user query information from that data set the server then homomorphically computes an encryption of query and send back the cipher text back to the user. In this technique the data and query is fully encrypted and privacy of user is maintained throughout the process.

DDoS attack on cloud is a very common security issues which is described in the last section. To protect cloud form this attack Intrusion Detection Systems (IDS) are developed. Author of [15, 16] explain that intrusion detection is basically a process of monitoring the network flow and analyze every packets to check any attempt of intrusion which violate the integrity, availability or confidentiality of the system. Mohamed et al. proposed collaborative IDS which will work on the IaaS layer of cloud and at the same time prevents the cloud from attack. Modi et al. in [17] proposed another IDS using the Snort and signature algorithm. The proposed framework captured packets from network and compares it with a known attack pattern and if packet give negative result then it allows the packets or else it follows the rules [17].

Authentication of users is done using digital signatures in a combination of SSO (Single Sign-On) and Ldap [11] Shibboleth is now used for web SSO to identify and grant access to the users across or within the organizational boundary. Access control mechanism is largely used in a fully shared system to give permission to the users' to access resources. Data dispersal storage and secure retrieval scheme [18] is one of well discussed approach. The suggested algorithm efficiently reduces some of privacy risk such as server colluding and unauthorized data modification. In the working scenario the system assigns users' data to various domains using some flexible distributed algorithms to maintain the integrity of the data.

5 Service Level Agreement in Cloud

Privacy is still a long-standing topic in Cloud. In cloud privacy, Service level Agreement (SLA) represents an important document which serves as contract between a user and a provider to deliver services. SLAs should cover performance,

reliability, and security and privacy of data and on this pre-defined contract the provider is bound to provide the service [19]. Any violation of SLAs will lead to a penalty that can be either monitory or anything other. Various issues that are included in SLA, introduces the following challenge in maintaining privacy:

- Storage—The main concerns are if the stored data is getting mixed with other data from other organization. Another important concern which makes user to think twice before storing confidential data in cloud is that if providers have the right to see the data without notifying the organization.
- Retention—One of the key question that organization needs to know is how long a service provider keeps the data in there server and how the ownership of the data is evaluated.
- Deletion of Data—To provide availability of data all the time cloud providers need to replicate the data. The main concern is, once the data retention period is over, how the user will make sure that all the replicated copies of the data are destroyed.
- Privacy breaches—If a breach occurs how the providers will notify the user and locate who is actually responsible for the breach?

SLA metric is constructed from a few common elements such as name of metric, metric source, duration of sampling, frequency of sampling, scope of testing, target range, weight, reporting process, and penalty/incentive calculation. These elements should be found with every SLA metric used to demonstrate services have been sustained to mutually agreed obligations [20]. Some general metrics are throughput, QoS, bandwidth etc. But SLA can also include some other metrics on the security perspective as it is a contract between user and provider and the users' concern on the data privacy can also be a point which includes security mechanism, security effectiveness as a metrics. The main concern for the user is to know how exactly the CSP deals with their private data. It is quite uncommon for a CSP to specify the security levels for user data associated with their services, hence impeding users from making data security relevant informed decisions. This is known as Quality of Protection (QoP), which includes the capability of a service provider to deliver service according to the security requirement of the user and how well the provider meets the requirements [21, 22].

6 Security SLA

Like SLA there is Sec-SLA (Security Service level agreement), which defines matrices related to security. A Sec-SLA should include [23]:

- Some description of the user required services that the provider is going to provide.
- All the security requirements, along with the monitoring process, which the user and provider are agreed upon before committing

- A detail process of reporting problems, threats or security breach incidents that may arise during the contract period
- Lists of penalties in case any of the party breaks the agreed SLA. This penalty can be either service credit or financial compensation. CSPs may also include restrictions on customer activities and also state some specific moments when the agreement do not apply.
- All the legal and regulatory matters that might happen during the time span which include references to existing legislations and directives that may affect the service as well as the terms under which the SLA will not be valid (Table 2).

In [22] authors had described a life cycle of Sec-SLA which consists of six steps. As security is a very vast portion and it depends upon different user specification so the negotiation between the user and provider is an important part. To create a Sec-SLA there are three steps to follow [18]

- Policy analysis
- Architecture analysis
- Interviews

With the above procedures the provider will evaluate the customer's requirements of web servers, systems and security policy that he will need during the contract period. The authors of [24] introduce the matric on which the negotiation can be done. Services delivered in an "On Demand" condition, require extensive effort in defining security matrices. In traditional SLAs, matrices are mainly QoS, Bandwidth and some portion of security as well. But in Security-SLA the matrices are for example Backup policies, Password management, Secure Network Protocols and Data Transport, data deletion effect etc. [24], which will ensure that the data are stored and also in control of the user. Even after negotiation the users are always worried about the implementation of the agreed security mechanism. To provide user with a privacy management tool the SLA must have been written in a machine readable language. WS-Agreement is a protocol for defining SLAs between

Table 2 User requirement for security in cloud

Level	Layer	Security requirements
Application level	SaaS	• Privacy in multitenant environment • Access control • Software security • Service availability
Virtual level	PaaS and IaaS	• Application security • Virtual cloud protection • Communication security • Management control security • Data security
Physical level	Datacenters	• Hardware security • Network protection • Network resource protection

providers and users [23]. Using this protocol the privacy management tool will help the user to control the storage of data and also modify the security on a move. This tool will help the user to negotiate the security without meeting the provider personally.

7 Future Work and Conclusion

Prospect and existing customers of service providers are demanding confidentiality, integrity, and availability when contracting with vendors for cloud computing [20]. As we are using more and more cloud based services in our daily life, we are giving and storing our information to the vendor side which can be accessed through internet. This paper mainly focuses on the vulnerabilities in cloud with some detail discussion on attacks and challenges faced by cloud technology in the recent times. We have also introduced Sec-SLA and matrices as an approach to help user to secure their personal data in cloud. Security SLA matrices are a medium to gain trust over the user and reduce risk. These matrices must be meaningful and economic cause creating a metrics includes computational cost. Irrelevant metrics can cause and impact on the quality of service by using excessive computational resources [20]. From the above discussion we can see that both the parties are liable to protect their personal information. But CSPs do not include anything in SLA about the security mechanism they are going to provide to their tenants. Apart from this there are few monitoring tools which can be used by the end user to monitor the security measures and at the same time this tool will help them to enforce new security features on their data [25]. Several outstanding issues exist related to cloud security and privacy. Security SLA is still in its early stage. Future research should focus on providing a full view of security that will offer to user and details about the data they stored in the cloud. Along with this there must be a web based framework that will negotiate SLA metrics dynamically and incorporate security according to the user instruction and at the same time give an overview to the vendor as well as user about the performance achieved by the provider. Apart from this there should be another part for further development that can be an extension of the framework which provides an opportunity to view the location of the data stored in the cloud by using meta-data information of the user data. There need to be more specific and detailed research work carried out to make security as a user centric approach, and provide a monitoring and modification tool to help user to choose their security requirement without any human intervention.

References

1. Y. Jadeja and K. Modi, "Cloud computing - concepts, architecture and challenges," in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, 2012, pp. 877–880.
2. G. Zhang, Y. Yang, X. Zhang, C. Liu, and J. Chen, "Key Research Issues for Privacy Protection and Preservation in Cloud Computing," in *2012 Second International Conference on Cloud and Green Computing*, 2012, pp. 47–54.
3. S. Hamouda, "Security and privacy in cloud computing," *2012 Int. Conf. Cloud Comput. Technol. Appl. Manag.*, pp. 241–245, Dec. 2012.
4. S. Surianarayanan and T. Santhanam, "Security issues and control mechanisms in Cloud," *2012 Int. Conf. Cloud Comput. Technol. Appl. Manag.*, pp. 74–76, Dec. 2012.
5. H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Secur. Priv. Mag.*, vol. 8, no. 6, pp. 24–31, Nov. 2010.
6. Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *J. Internet Serv. Appl.*, vol. 1, no. 1, pp. 7–18, Apr. 2010.
7. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, Oct. 2012.
8. S. M. Rahaman and M. Farhatullah, "PccP: A model for Preserving cloud computing Privacy," *2012 Int. Conf. Data Sci. Eng.*, pp. 166–170, Jul. 2012.
9. S. De Capitani Di Vimercati, S. Foresti, and P. Samarati, "Managing and accessing data in the cloud: Privacy risks and approaches," *7th Int. Conf. Risks Secur. Internet Syst. Cris. 2012*, 2012.
10. K. Surya, M. Nivedithaa, S. Uma, and C. Valliyammai, "Security issues and challenges in cloud," *2013 Int. Conf. Green Comput. Commun. Conserv. Energy*, pp. 889–893, 2013.
11. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.
12. P. Yadav and S. Sujata, "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA," *Int. J. Cloud Comput. Serv. Archit.*, vol. 3, no. 3, pp. 25–40, 2013.
13. I. Roy, S. T. V. S. T. V Setty, A. Kilzer, V. Shmatikov, and E. Witchel, "Airavat: Security and privacy for MapReduce," *Proc. 7th USENIX Conf. Networked Syst. Des. Implement.*, pp. 20–20, 2010.
14. D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *2012 Int. Conf. Comput. Sci. Electron. Eng.*, vol. 1, no. 973, pp. 647–651, 2012.
15. M. P. K. Shelke, M. S. Sontakke, and a D. Gawande, "Intrusion Detection System for Cloud Computing," *Int. J. Sci. Technol. Res.*, vol. 1, no. 4, pp. 67–71, 2012.
16. H. Mohamed, L. Adil, T. Saida, and M. Hicham, "A collaborative intrusion detection and Prevention System in Cloud Computing," in *2013 Africon*, 2013, pp. 1–5.
17. C. N. Modi, D. R. Patel, A. Patel, and M. Rajarajan, "Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing," *Procedia Technol.*, vol. 6, pp. 905–912, 2012.
18. L. Chen and D. B. Hoang, "Novel Data Protection Model in Healthcare Cloud," in *2011 IEEE International Conference on High Performance Computing and Communications*, 2011, pp. 550–555.
19. H. Tianfield, "Security issues in cloud computing," *2012 IEEE Int. Conf. Syst. Man, Cybern.*, pp. 1082–1089, Oct. 2012.
20. M. Hoehl, "Proposal for standard Cloud Computing Security SLAs - Key Metrics for Safeguarding Confidential Data in the Cloud.".
21. R. Schmidt, "Conceptualisation and Lifecycle of Cloud Based Information Systems," *2012 IEEE 16th Int. Enterp. Distrib. Object Comput. Conf. Work.*, pp. 104–113, 2012.

22. K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Security SLAs for Federated Cloud Services," in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011, pp. 202–209.
23. M. Jaatun, K. Bernsmed, and A. Undheim, "Security SLAs–An Idea Whose Time Has Come?," *Multidiscip. Res. Pract. Inf. Syst.*, pp. 123–130, 2012.
24. S. A. de Chaves, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing," in *2010 Sixth International Conference on Networking and Services*, 2010, pp. 212–217.
25. M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, and U. Villano, "Security as a Service Using an SLA-Based Approach via SPECS," *Requir. Eng. Cloud Comput. (RECC - CloudCom)*, vol. 2, pp. 1–6, 2013.