Cloud Forensics: A Framework for Digital Forensic in Cloud Based Environment by Identifying SLA Breaches by Cloud Actors

Sulabha Patil[1], Rajiv Dharaskar[2], Vilas Thakare[3]

[1]*Department of Computer Science & Engineering, Amravati University, India*
[2]*Director, MGI, Nanded, India*
[3]*HOD, Department of Computer Science & Engineering, Amravati University, India.*

Abstract: **Cloud Service Provider(CSP) and Cloud Service Consumer(CSC) work on the terms agreed in the Service Level Agreements(SLA). SLA is a written agreement which serves as the basis for the expected level of service the CSP must provide. As the CSP are enterprises that are profit driven it is beneficial for the CSP to cheat on the SLA. Hence CSP do not provide the facility of auditing the SLA. As such the CSC must be equipped to ensure that the services promised by the CSP are provided by it so that in case of breach of service, the CSC has sufficient evidences to claim for penalty. Moreover virtual machines are prone to attacks by malicious cloud actors. To aid the investigation process sufficient evidences are needed. Hence, a framework based on the concept of Third Party Auditor (TPA) is proposed in this paper. This TPA will be placed between the Cloud Service Provider (CSP) and the Cloud Service Consumer (CSC) to closely monitor terms and conditions of SLA and ensure that CSP satisfies all the conditions mentioned in the SLA. If it is violated then the framework detects and stores it in a database maintained for this purpose. The TPA will also monitor attempts by malicious cloud actors and maintain log of all such attempts. Snapshots of clients' virtual machines will also be stored at a regular interval.**

Keywords**: CSP, CSC, SLA, TPA, SLO**.

I. INTRODUCTION

Emergent use of computing and digitization is responsible for the evolution of new discipline named digital forensics. Digital forensics in cloud computing brings new technical and legal challenges due to remote and scattered data. According to [19] data centre of cloud environment are attacked by various types of attacks such as DoS, DDoS, sniffer attack, spoofing, phishing, Non-repudiation. However it is possible to trace for evidences in cloud environment based on the logs generated by the user during interaction with the cloud service provider. The interaction of the Cloud Consumer with the CSP is through the internet browser and hence network logs can be utilized as evidences in forensic investigations. Many authors have devised methodologies to utilize these logs for generating forensic evidences. Whenever an enterprise or a user wish to utilize cloud services they have to undertake a Service Level Agreement with the Cloud Service Provider. Both the parties are bounded to each other via this agreement commonly referred to as SLA. In this paper we are proposing a framework for digital forensic in cloud computing environment. An auditor based system will monitor transaction between the Cloud Service Provider and Cloud Consumer and maintain a database of all these transactions. Besides this, database of security breach by the consumer and by the provider will be maintained in independent database. Section II give the review of the background. Section III deals with Review of breaches by the CSP, Section IV deals with Proposed methodology and Section V deals with Conclusion and Future work.

II. BACKGROUND

As per Amirullah Amirullah et.al. [1] two places can be searched in cloud for getting probable evidences, the first is the browser used and the second is the application installed in user's device. Various information is available which can be used as evidences, to name some of them is the user details, logging information, files accessed etc.

Emi Morioka, et.a. [2] suggests that amongst the three models of cloud, IaaS provides greater access to user as compared to SaaS and Paas. Hence, in case of SaaS client, the only hope to get data for forensic investigation is the web browser on the client side . File fragments and web cache that are left in the local system must be extracted as far as possible. Audit control node at the Internet Service provider is the another place where interaction between client and cloud takes place. It is mandatory on the part of the ISP to comply with the rules and regulations laid down. Hence control nodes of the ISP are one of the objects which should be investigated.

According to Mohit Soni et.al [3] One key aspect of Digital forensic is to be able to produce evidences of the crimes carried out using digital media so that they can be presented in the court of law. Network Logs are important evidences. A Generic framework is proposed for carrying out forensic analysis of live network. Networking module is defined using a open source software named OpenContrail which is integrated with Openstack framework. This combination provides strong connectivity. Pay per use model is implemented for economic viability of the model for users and service providers.

As per Mahmoud M Nasreldin et. Al [4] in network security the regular approach of achieving message confidentiality and authenticity is to sign the message and then encrypting it with its signature. Normally the sender signs the message using a digital signature scheme and then appropriate encryption algorithm is used for its encryption. Usually private key encryption algorithm is used. Recipient's public key is used for encryption of random message key. This is a two step approach i.e., sign and then encrypt or encrypt then sign. But both these scheme are vulnerable to attacks such as plaintext subsection and Forwarding attacks and cipher text stealing attacks.

To overcome these issues a three block approach i.e. Sign-Encrypt-Sign or Encrypt-Sign-Encrypt is proposed by authors. Cryptographic algorithms are used for ensuring confidentiality, authenticity and integrity.

For several years use of VM for creation of contained environments was made this was done for examination of suspect devices or for isolation of malware. However, now VM have themselves become target for examination and investigation. Moreover in order to get snapshot details and contents and metadata related to it, the examiner must have host privilege. Author at [5] suggest a methodology that will help in acquisition of memory data without the intervention of the CSP and acquisition of contents of snapshots without changing it to any other file format so that it can be presented as a evidence in the court.

Valentina Casola et.al[6] has proposed a system named security-by-design in clouds. Here a security – SLA driven methodology has been proposed to build secure cloud applications.

Authors at [7] proposed an ontology based approach for gathering digital evidences in cloud environment. Cloud belongs to distributed architecture, hence traditional approach of digital forensics cannot be applied to it directly. In cloud computing environment most of the forensics data is generated from data logs and their comparison pre and post attack. However manual comparison of these logs is a very tedious and next to impossible task considering quantum of logs generated. Hence an automated system is proposed.

Service Level Agreement is the most important document in cloud computing environment. It is signed between Cloud Service Provider (CSP) and Cloud Consumer for ensuring legitimate use of cloud computing environment on the part of user and for ensuring delivery of artifacts promised on the part of the CSP. According to [8] due to legal and ambiguous terms in SLA several conflicts and issues exists in the process of negotiation of SLA. Application of semantic knowledge during formation and negotiation of SLA can resolve this issue. Thus a Semantic Web Platform using ontology is designed and evaluated.

Several difficulties are faced by the service provider who are hosting data centres. To deliver hosted services which are SLA compliant SaaS provider have to satisfy minimum service level of customer that too in a less cost. In order to achieve this he has to maintain balance between available resources and users demand. This task becomes more tedious because of factors such as (a) heterogeneity in resource allocation (b) mapping of user requirements to available infrastructure (c) management of dynamic changes of customers. To overcome these issues authors at [9] have proposed a framework that ensures allocation of resources avoiding SLA violation in SaaS.

In order to surmount difficulties faced by SaaS provider discussed above R.S. Mohana et.al[10] suggests an admission control and scheduling algorithm based on machine learning approach for SaaS provider. This will enable them to effectively utilize public cloud resources to maximize profit on one hand and achieving customer satisfaction and minimizing cost on the other.

III. REVIEW OF SLA BREACHES BY CLOUD SERVICE PROVIDERS

The SLA is the legal term a legal umbrella, under which one or more Service Level Objective(s) (SLO) exists [18]. These SLOs describe the services, measurement methodology such as availability, performance, security and compliance/privacy and objective (uptime, speed, transaction / seconds, etc.). SLA is executed to fulfill Service Level Objectives (SLO), these SLO are evaluated according to measurable Key Performance Indicators (KPIs).

Authors at [12] states that in April 2011 there was an outage of four days for Amazon cloud but still it did not breach Amazon's EC2 SLA. How ? the SLA "guarantees 99.95% availability of the service within a Region over a trailing 365 period." Now the servers that failed were EBS and RDS rather than EC2 itself and these failures were restricted to Availability Zones within single region, legally speaking the SLA was not breached.

SLA serves as the basis for the expected level of service the CSP must provide. As the CSP are enterprises that are profit driven it is beneficial for the CSP to cheat on the SLA. Hence CSP do not provide the facility of auditing the SLA. To resolve this issue, the burden of auditing the SLA is shifted to the user by Amazon EC2[11]. But overhead for carrying out such audit on the part of the individual user is high because auditing will consume resources for which user has paid.

Under all these circumstances the only option remains is to allocate the task of auditing the SLA onto the third party whose sole purpose is to verify that the terms and conditions mentioned in the SLA are being met. But in this method also the CSP can interfere with the auditing process that is being carried out by providing forged data.

In [13] authors have proposed an algorithm which carries out auditing of the CPU allocation and simultaneously verify that the corresponding SLA is met. For carrying out this verification a SLA verification framework is suggested. This framework makes use of a Third Party Auditor (TPA). Authors claim that using the TPA, it can be provided that the CSP satisfies all the conditions mentioned in the SLA or if it is violated then the framework detects and reports it. But in this paper authors have restricted the audit to the SLA of the IaaS provider and that too only single parameter of CPU allocation is considered.

A review of breaches that may occur on the part of the provider and on the part of user is presented herein.

Table I
Details of probable breaches of SLA by the CSP and CSU

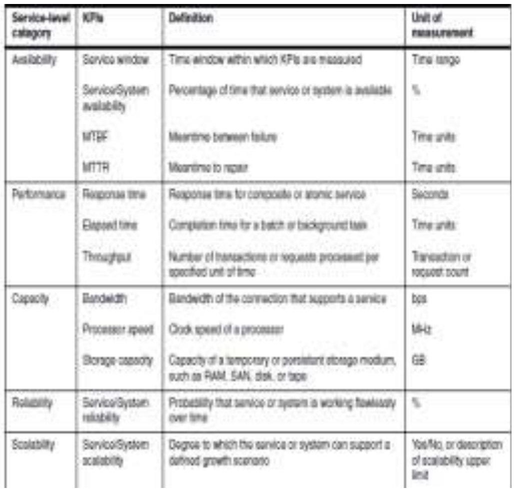
Description of Probable breaches by C.S.P. if the clauses are mentioned in the SLA	**Description of probable breaches by the C.S.C.**
Violation of Intellectual Property rights	Uploading of unlawful, obscene, offensive or fraudulent content or activity amounts to breach of SLA as it is the primary clause mentioned in any of the SLAs.
Failure to provide security to data in the form of encryption and other methods.	Interfering with or violating the integrity of data or services by Monitoring or Crawling or causing Denial of Service (DoS);
Transferring data to other locations without informing the user about it. This may affect the security and privacy policy as it varies from nation to nation and region to region.	Interfering in security of a network or system. Intentional Interference; Avoiding System Restrictions.”
CSP not providing reports of penetration testing or security audits, is committing a breach of service.	Evading filters,
Appointing a sub contractor for administrative activity without the knowledge of user. User have the right to know whether this subcontractor is applying the same level of security as that promised in SLA.	Sending unsolicited, abusive or deceptive messages viruses or harmful code
CSP must disclose measures about his own personal access to users Personal Identification Information eg. Data related to customers when the CSU is a bank.	Unauthorized Access;
Non- disclosure of such measure terms of breach of service.	
CSP must notify provider the location i.e., countries where data will be stored. If User restricts some countries that must be followed by the CSP.	Falsification of Origin.
CSP suddenly decides to stop his services without following proper exit procedure.	Alter or obscure mail headers
If there is a mention of patch up of O.S. and its maintenance and updating of software clause for protection from vulnerabilities, the CSP must mention the interval of such update. Failing to follow this clause amounts to breach.	

As shown in the Table No.1, there are numerous incidents wherein breaches can occur. There is a need to identify such breaches and to collect sufficient evidences so that they can be presented while claiming penalties.

There are four categories into which a SLA can be divided. Service related elements, agreement related elements, document related elements and management related elements [19]. In this project we are interested in service-related elements. These elements explains the manner in which the service is regulated. It describes what, when, who and where about the services that are provided.

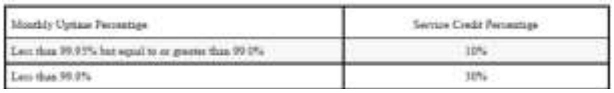
Contents of SLA are different for different delivery models i.e. , IaaS, PaaS and SaaS. As mentioned above SLAs are based on SLOs and they can be measured by the Key Performance Indicators (KPIs) which are nothing but the metrics provided for analysis of the services provided by the CSP. Cloud Service level categories and the key performance indicators related to it are displayed below in Table No.2 [20].

Table II
Cloud Service level categories and related Key Performance Indicators



Service-level category	KPIs	Definition	Unit of measurement
Availability	Service window	Time window within which KPIs are measured	Time range
	Service/System availability	Percentage of time that service or system is available	%
	MTBF	Meantime between failure	Time units
	MTTR	Meantime to repair	Time units
Performance	Response time	Response time for composite or atomic service	Seconds
	Elapsed time	Completion time for a batch or background task	Time units
	Throughput	Number of transactions or requests processed per specified unit of time	Transaction or request count
Capacity	Bandwidth	Bandwidth of the connection that supports a service	bps
	Processor speed	Clock speed of a processor	MHz
	Storage capacity	Capacity of a temporary or persistent storage medium, such as RAM, SAN, disk, or tape	GB
Reliability	Service/System reliability	Probability that service or system is working flawlessly over time	%
Scalability	Service/System scalability	Degree to which the service or system can support a defined growth scenario	Yes/No, or description of scalability upper limit

CSP follows metrics given by them in SLA for example Amazon EC2 and EBS [14] mentioned monthly uptime percentage and the service credit percentage as follows :



Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0%	30%

IV. PROPOSED METHODOLOGY

As per [11], all the CSP rely on customers to ensure that the SLA is followed. SLAs are prepared by the CSP hence all the clauses are in favour of the CSP and the responsibility of following it lies with the cloud customer. There are various parameters on which the services of the provider can be judged. Eg. Downtime percentage, Credits, response time, server availability, network availability. Analysis and review presented herein states that almost all SLAs mention that customer must take specific action before claiming such credits on the CSP. Specific action are as follows :

- Customer must identify and report failures.
- The timeframe for reporting may differ , it may be 48 hours, 7 working days, 15 days, after the end of the billing cycle in which the errors was observed.
- It is mandatory on the part of Customer to provide the “proof” of breach which includes dates/times, request logs of servers, trace routes, complete description of service interruption, the duration of the interruption and names of affected databases and failed operations, etc. in the case of PaaS SLAs.

In order to maintain the record of above issues, and also to keep track of malicious activities that may take place on the client machine we are proposing a generic framework based on Third Party Auditor which will audit the SLA executed between the Cloud Service Provider and the Cloud Consumer and will audit different parameters such as downtime percentage, credit, logs of transactions between the CSP and Cloud customer.

Moreover if intruder tries to intrude upon the clients machine all such activities will also be recorded. Snapshots of the clients machine will be maintained at regular intervals so that all these logs and databases can be produced as evidences. TPA will be an independent authority who will be maintaining different databases in order to have a close watch on all the transactions that are being carried out by the Client machine. The databases that will be maintained by the TPA are :

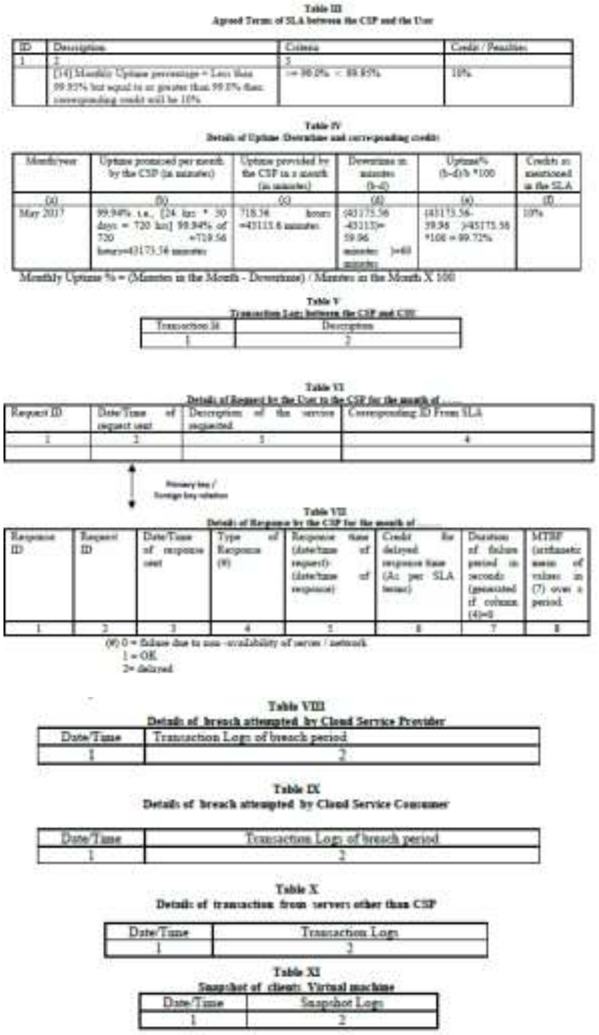


Table III
Agreed Terms of SLA between the CSP and the User

ID	Description	Criteria	Credit / Penalties
1	2	3	
	[14] Monthly Uptime percentage = Less than 99.95% but equal to or greater than 99.0% then corresponding credit will be 10%	>= 99.0% < 99.95%	10%

Table IV
Details of Uptime Downtime and corresponding credits

Month/year	Uptime promised per month by the CSP (in minutes)	Uptime provided by the CSP in a month (in minutes)	Downtime in minutes (b-d)	Uptime% (b-d)/b *100	Credits as mentioned in the SLA
(a)	(b)	(c)	(d)	(e)	(f)
May 2017	99.94% i.e., [24 hrs * 30 days = 720 hrs] 99.94% of 720 =719.56 hours=43173.36 minutes	718.56 hours =43113.6 minutes	(43173.36 -43113)= 59.96 minutes)=60 minutes	(43173.36- 59.96)/43173.36 *100 = 99.72%	10%

Monthly Uptime % = (Minutes in the Month - Downtime) / Minutes in the Month X 100

Table V
Transaction Logs between the CSP and CSC

Transaction Id	Description
1	2

Table VI
Details of Request by the User to the CSP for the month of ....

Request ID	Date/Time of request sent	Description of the service requested	Corresponding ID From SLA
1	2	3	4

Table VII
Details of Response by the CSP for the month of ....

Response ID	Request ID	Date/Time of response sent	Type of Response (#)	Response time (date/time of request)-(date/time of response)	Credit for delayed response time (As per SLA terms)	Duration of failure period in seconds (generated if column (4)=0	MTBF (arithmetic mean of values in (7) over a period
1	2	3	4	5	6	7	8

(#) 0 = failure due to non -availability of server / network
1 = OK
2= delayed

Table VIII
Details of breach attempted by Cloud Service Provider

Date/Time	Transaction Logs of breach period
1	2

Table IX
Details of breach attempted by Cloud Service Consumer

Date/Time	Transaction Logs of breach period
1	2

Table X
Details of transaction from servers other than CSP

Date/Time	Transaction Logs
1	2

Table XI
Snapshot of clients Virtual machine

Date/Time	Snapshot Logs
1	2

An application is developed which will monitor parameters that are to be audited and which are mentioned in the SLA. Eg. Uptime / Availability % or credit eg. 5% of fees for each 30 minutes of downtime, etc. Tasks that will be performed are as follows :

1) Extraction of SLOs, measures, penalties mentioned in the SLA and update the database. Technical person from the CSC’s team is capable of extracting all the metrics from the SLA and updating the database.
2) Monitoring transactions between CSP and CSC and updating relevant database.
3) Evaluation of services provided during one billing month against the services promised.
4) Calculation of penalties if any on the basis of agreed terms.
5) Generating transaction logs wherever penalties are calculated so that they can be submitted by the CSC as evidence while claiming the penalty from the CSP

6) Creation of a scenarios for attacking clients virtual machine by DDoS and Brute Force Attack.
7) Maintaining Logs of all such attacks.
8) Taking snapshots of clients' virtual machines at a regular interval and maintaining it in database.

As per [12] Some of the common performance metrics are throughput i.e., response speed of the system, reliability which means the availability of the system. load balancing, durability, elasticity, linearity i.e., system performance with the increase in the load, agility which reflects the quickness with which the provider responds to changes in load automation i.e., percentage of requests handled without human interaction and customer service response times.

Besides these other metrics are Mean Time Between Failures (MTBF) (arithmetic mean of the intervals between failures over a period of time), Mean Time to Recover (MTTR) (the arithmetic mean of time elapsed between recovery and next failure) and Mean Time to Failure (MTTF) is the difference between MTTR and MTBF.

Of all the metrics discussed above, our system will be auditing on :

a) Uptime /Downtime % and calculating credit % accordingly
b) Customer response time
c) Mean Time Between Failures (MTBF)
d) Transaction logs between cloud service provider and cloud service customers
e) Logs for breach of SLAs by the CSP
f) Maintaining Logs of all attacks and
g) Maintaining snapshots of clients' virtual machines at a regular interval in database.

All these parameters will be stored in a separate database which will be maintained with the TPA. Our Application will check if MTBF exceeds the limit mentioned in the database and include it in the table of breach. Similarly the application will keep close watch on the date and time of the requests made and the response given by the provider. If the difference between the response time and request time is more than the agreed terms of SLA, a breach on the part of the provider will be recorded in the appropriate database.

Above framework will be implemented on three different cloud service providers namely Znet windows, Godaddy Linux vpa and Aws Linux. Local Virtual machine will be used to demonstrate the working.

V. CONCLUSION AND FUTURE SCOPE

The Digital Forensics Framework proposed in this paper will be helpful in providing evidences of SLA breach by the cloud service provider. It will also maintain transaction logs and snapshots of the virtual machines so that these can also be provided to the investigator for carrying of forensic analysis in case of malicious attack on the client's virtual machine.

The framework proposed in this paper have considered 3 parameters to assess the breaches by the cloud service providers and only two types of network attacks are considered. More network attacks can be traced and transaction logs of those attacks can be generated in the future work.

REFERENCES

[1]. Amirullah Amirullah, Imam Riadi, Ahmad Luthfi, "Forensic Analysis from Cloud Storage Client Application on Proprietary Operating System", International Journal of Computer Applications(0975-8887), Vol. 143-No.1, pp. 1-7, 2016.
[2]. Emi Morioka. Mehrdad S Sharbaf, "Cloud computing : Digital Forensics Solutions", 12th International Conference on Information Technology-New Generations, 2015.
[3]. Mohit Soni, Manish Kumar Bharti, Frass: A Framework for Digital Forensic Services in a Cloud-based Environment, The International Journal of Forensic Computer Science, IJOFCS, pp.15-22, 2015.
[4]. Mahmoud M Nasreldin, Magdy El-Hennawy, Heba K. Aslan, Adel El-Hennawy, "Digital Forensics Evidence Acquistion and Chain of Custody in Cloud Computing", International Journal of Compuer Sciences Issues, Volume 12, Issue 1, No 1, 153-160, January, 2015.
[5]. Sameera Almulla, Youssef Iraqi, Andrew Jones, "Digital Forensic of a Cloud Based Snapshot", IEEE sponsored International Conference on Innovative Computing Technology, (INTECH 2016), 724-729, 2016.
[6]. Valentina Casola, Alessandra De Benedictis, Massimiliano Rak, Erkuden Rios, "Security-by-design in clouds: a Security-SLA driven methodology to build secure cloud applications", Procedia Computer Science 97, 53 – 62, 2015.
[7]. Suchana Datta, Chandan Pan, "An Intelligent Forensic Framework towards Cloud: Its Ontological Aspects", International Journal of Computer Applications, 2016.
[8]. Dr. K. Saravanan1, Dr. S. Silas Sargunam2, Dr. M. Rajaram, "An Automated Semantic Negotiation for Cloud Service Level Agreements", Circuits and Systems, 7, 2443-2451, 2016.
[9]. Shantanu Sasane Abhilash Bari Kaustubh Memane Aniket Pathak Prof. A. A.Deshmukh, "Resource Allocation Avoiding SLA Violations in Cloud Framework for SaaS", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 1, 3091-3094, January – 2014.
[10]. R.S. Mohana And P. Thangaraj, "Machine Learning Approaches in improving Service Level Agreement-Based admission control for a Software-As-A-Service provider in cloud", Journal Of Computer Science 9 (10): 1283-1294, 2013.
[11]. Cloud Standard Customer Council's Public Cloud Service Agreements: What to Expect and What to Negotiate Version 2.0.1 , August 2016,
[12]. Service Level Agreements in the Cloud: Who cares? www.wired.com/insights/2011/12/ service-level-agreements-in-the-cloud-who-cares/
[13]. Ryan Houlihan, Xiaojiang Du, Chiu C. Tan, Jie Wu, Mohsen Guizani, "Auditing Cloud Service Level Agreement on VM CPU Speed", IEEE ICC Communication and Information Systems Security Symposium, pp.799-803, 2014.
[14]. Amazon EC2 Service Level Agreement: http://aws.amazon.com/ec2/sla/
[15]. Amazon S3 Service Level Agreement: http://aws.amazon.com/s3/sla/

[16]. Dimension Data Service Level Agreement: http://cloud.dimensiondata.com /am/en/about /legal/service-level-agreement

[17]. Future Hosting Service Level Agreement: www.futurehosting.com/legal/dedicated-service-level-agreement

[18]. A practical Guide to SLA, Performance and Operation, August, 2016, http://blog.catchpoint.com/2016/08/04/sla-practical-guide/

[19]. Stefan Frey, Claudia Luthje, Christoph Reich, "Key Performance Indicators for Cloud Computing SLAs, The Fifth International Conference on Emerging Network Intelligence, 2013, ISBN:978-1-61208-292-9, pp. 60-64.

[20]. Performance Implications of Cloud Computing, a red paper by IBM, Copyright IBM Corp. 2012. All rights reserved. ibm.com/redbooks 1

[21]. Sulabha Patil, Uzma Ali, R.V.Dharaskar, "Design and Development of System for detection of security Breach in Cloud Environment", International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782 (Online) Volume 3, Issue 9,pp, 221-227, September 2015.