Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-46

Cloud Computing

Security Issues and Measures

Aniruddha S. Rumale[1*], Dr. Dinesh N. Chaudhari[2]

Abstract— **Cloud computing is advanced distributed and parallel processing, involving Grids, clusters, virtualization of resources, networking, client-server mechanism etc… Without proper security such an integrated complex system won't last for long. This paper briefs out types of security issues that a cloud must consider before and after its implementation. Service Level Agreements (SLA) plays an important role in cloud operation and implementation, as it covers almost every aspect of cloud. Paper discusses on what a clouds SLA must contain, and why SLA can't be implemented from users' point of view. Paper discusses in brief the security in/for/by cloud scenario of cloud computing. Paper discusses existing methods/measures for security and can be seen as a brief on cloud computing security issues and measures. This paper can act as a theoretical base or directives while designing and implementing the cloud as it briefs out information on cloud security.**

Keywords— Security in cloud, Security for cloud, Security by cloud, Trusted cloud computing, Security issues in cloud, service level agreements

I. Introduction

Cloud computing promises high performance solutions to everyday problems of individuals as well as organizations, by providing them necessary Infrastructure, platforms, software, etc, as services. Cloud Computing reduces cost of hardware and software ownership and maintenance, to allow companies to focus on their core business strengths. There is no all-inclusive definition for cloud computing, but, as per the NIST [1, 2] the cloud computing is defined as

"A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service level agreements established through negotiation between the service provider and customers and can be ubiquitously accessed from any connected devices over the internet." [3–6]

Cloud computing involves high performance data-centers, networks and communication systems, high performance processing hardware and other resources. No system becomes effective and efficient without effective and efficient design and its implementation requires taking care of any and all threats or situations, which can compromise the reliability, effectiveness, and efficiency of the system and can affect its working drastically either from users' point of view or from systems point of view. This means providing security to, and securing the system. Cloud computing need to be secure and trusted, else it can't be effective and efficient.

Cloud-computing uses existing networks for providing its services on 'pay per use basis' to cloud-user [3, 5, 7,9-12]. So the threats that are possible in existing networks must be taken care of while implementing cloud computing. Cloud computing is highly distributed and parallel in nature, means security threats that are possible in distributed and parallel computing are readily available to cloud computing and must be taken care of at the time of cloud implementation. Cloud offers services to its users on pay per use basis, this involve right billing and some legal contracts between cloud-providers and users; usually called as Service level agreements(SLA)[8]. Thus cloud computing requires every bit of security measures to be considered while implementing it and have all sort of security issues to answer or resolve at the same time. Cloud computing provides the capability to use computing and other resources on a metered basis and reduce the investments in an organizations computing infrastructure [12, 13].

In this paper, SectionI, introduces cloud computing. SectionII talks on the types of cloud computing. SectionIII briefs out the service level agreements (SLA). SectionIV discusses various types of security issues in cloud computing. SectionV briefs out the Security Threats & remedial measures.

II. Cloud Computing Models

Three main delivery models of cloud computing are

1) Infrastructure as a Service(IaaS), in this type the basic infrastructure, like data storage, computational hardware, Networks etc, are provided on metered basis to the user. IaaS frees the cloud user from installing and maintaining ones own infrastructure.

2) Platform as a Service(PaaS), in this type the basic platforms like some proprietary operating systems are

Aniruddha S Rumale[1*], Associate Professor
SVPMs COE, Malegaon-bk, Baramati, Pune University
Maharashtra, India -413115

Dr. Dinesh N Chaudhari[2], Dean Academics, Professor, & HOD Computer.
JDIET, Yavatmal, SGBA University, Amravati
India -445201

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-46

provided as service to the end user. PaaS helps cloud user to develop the applications for the various platforms or to work on various platforms without buying the license copies and required resources of that platform.

3) Software as a Service (SaaS), in this type the some software like proprietary multimedia suits, IDEs etc, can be used by the user without investing in them to develop some applications out of them or to carry out some work depending on them. [7, 14]

Four main deployment models of the cloud computing are

1) Public Cloud, in this, services to end users are made available through third party service provider via Internet. Every user given with a access code to enter or leave the cloud.

2) Private Cloud, here, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. It also provides more control to cloud-users as well as provider, as access is designated and always within the restricted network of the particular organization, which is deploying it. Private clouds generally uses Intranet or dedicated virtual private network(VPN).

3) Community Cloud, Community cloud is similar to that of private cloud, except the network used may not be owned by the community. These clouds exist due to shared or communal interests of participating persons or organizations.

4) Hybrid Cloud, is the mix of public and private cloud, where organizations usually keep their crucial information on private cloud and non-crucial information is made available to public / customers via public cloud. [7, 14]

III. Service Level Agreements

Service Level Agreements(SLA)[8],ideally plays a very important role in cloud operations, as cloud computing need to take care of many non-technical issues like local legal issues, business contract between cloud provider and user. Security and depth of security thus can be forced by the proper SLA [8]. In practice monitoring/verifying that SLA levels are respected by cloud-provider is difficult because it is usually the case that there is no opportunity to negotiate the contents of the agreement with the major cloud providers like Amazon, Google etc. They offer a standard set of terms and conditions and user generally have no power to force SLA-based security terms and conditions on the major providers. But, this approach can be used when implementing a private cloud. This won't cancel the significance of SLA based security in cloud, as many major providers already have a SLA based security drafts with below discussed features of SLA. (See Figure 1). Following issues makes SLA an important part of cloud computing.

(i) Integration: Cloud need to look for integration points with security and identity management technologies you already have, such as Active Directory, and controls for role-based access and entity-level applications. Proper integration promises better performance. Integration and its way need to be documented and agreed upon by the cloud provider as well as users for reliable implementation and constructing test benches for cloud computing services and security depth. Security depth means the type and extent of security measures that can be used to secure the cloud and its services. [8, 15]

Figure 1. Salient points to consider while drafting SLA

(ii) Privacy: A cloud service must include data encryption, effective data anonymization, and mobile location privacy. This is essential to be mentioned in SLA, as SLA gives a blueprint for what to add and what to deduct for providing privacy to user. Privacy providing mechanisms must need to obey the law and order of legacy system of the country of cloud provider as well as country of the cloud user; and that by not offending any international laws. Thus an ill documented SLA and privacy system implemented based on it can legally jeopardize the cloud provider and user. [15, 16]

(iii) Identity and access: A Cloud must have means to prevent inadvertent access. Cloud more often uses Internet for connectivity, which is having its own list of security threats. One risk of using Internet is the possibility of identity hijacking or theft. This, if not properly handled in SLA as well as in implementation, then the user may get compromised by some Cybergoon. A mechanism strong enough to safeguard the users account by not allowing any inadvertent access to it is desired. This can be achieved by using multilevel user authentication process and dynamic password generation with SSL(Secure Socket Layer) or like protocols. In authors view a VPN(Virtual Private Network) with right mix of multilevel authentication process can help here. [15, 16]

(iv) Compliance: Cloud must have vendor certification and compliance with industry and government standards that affect users' agency. As mentioned in point ii, cloud need to obey the legacy systems, both global and local for not to legally offend any party either cloud provider or cloud user. Total compliance with Industry and Government is required. [17]

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-46

(v) Service integrity: Cloud must protect software from corruption (malicious or accidental) and always ensure the security of the written code. Data compartmentalization and applying advanced encryption decryption mechanism to read/write data in cloud helps in security of written code. Cloud Computing being fully virtualized[18], must allow computers to be built from distributed components such as processing, storage, data, and software resources. Cloud Computing uses Service Oriented Architecture(SOA) [19], where server provides services to client and client(cloud-user) pay the charges for them to server(Cloud-service-provider).

Any corruption in any component or service of a cloud can kill the very purpose of the cloud. So, protecting the cloud components becomes a first priority for service integrity. This can be achieved by employing redundancy principle (keeping at least one exact up to date copy of whatever data/code is there on the cloud ; and providing at least one robust exact copy of the hardware/machines with same software(s) to carry out the work incase of failure of either). This also involves providing proper cooling and ventilation to heating cloud(servers) serving the users. Service integrity thus can be considered as soul of the cloud computing and a must part of any SLA. [15]

(vi) Jurisdiction: Location of cloud providers operation can affect the privacy laws that apply to the data it hosts. Does user's data need to reside within user's legal jurisdiction? Government records management and disposal laws may limit the ability of agencies to store official records in the cloud [20].

Principles of cloud (refer table I) itself require stringent SLA implementation. Table I points out that SLA must mentioned the way of resource pooling, virtualization, providing reliability and availability through elasticity and automation, and the measures to charge per use of a service, that is, billing schemes. Just mentioning these in SLA are not sufficient. It requires continuous monitoring and correct implementation of SLA. Thus, SLA plays very important role in secure cloud computing. SLA in every term provides details of design and implications of the implemented design; and proper implementation of SLA promises a secure and reliable Cloud to work with [8, 15, 16, 21].

IV. Security Issues

Cloud computing security can be classified in three aspects of security, viz, (a) Security in the Cloud, (b) Security for the Cloud, and (c) Security by the Cloud [7]. Refer figure 2.

A. Security in the Cloud

Data or information stored within cloud need to be kept secure. This can be achieved by (a) using advanced data encryption and decryption methods with data compartmentalization, whereby only the right owner and in exceptional cases cloud-provider can access the data. (b) using data-redundancy principle, by maintaining more than one copy of the same data it assures that data will be available at any given time. Security in cloud is very important to make the cloud trusted [5,6].

Data-redundancy is technique to keep your data safe and make it available at any given time whenever it is needed. Replication and refreshment of data is a core of data-redundancy principle. Redundancy principle can also be used for resources, so that even a resource in use fails, an alternate resource can be made available for carrying out the scheduled task.

In data redundancy popular technology is RAID (Redundant Array of Inexpensive Disks). Now a days generally used in either NAS (Network Attached Storage) or SAN(Storage area Network). In distributed systems, RAID principles can be used to replicate data across network nodes instead of using Array of disks to do so [7,18]. Data redundancy requires to take care of refreshment policy for replicated data; usually every backed up copy of data is refreshed/updated automatically after some predefined time interval if the number of copies to be updated are few. Some cloud operators' uses on demand updates; that is, updating when necessary. In this scheme alternate copies of data only get updated during the access time. Data-redundancy promises data availability and while data compartmentalization with encryption decryption promises data security.

Compartmentalization involves defining access right levels of the user and assigning different address spaces to each user so that no user can enter inadvertently into the other users account or can have any access to other users data. Because cloud can have any number of users using it at any given time, without compartmentalization of users and their data, cloud can not be called as secure and trusted. Compartmentalization of service simply mean that a service offered by cloud must have to be ubiquitously available to each user. No user while using the service of cloud, ever have to know that how many others are using the same service [13].

TABLE I
FIVE MAIN PRINCIPLES OF CLOUD COMPUTING

Resource	Explanation
Pooled resources	Resources like Infrastructures, Platforms, and Services are gathered and made available to any subscribing users.
Virtualization	High utilization of hardware assets or resources as none of them remain ideal because many subscribing users can use them at any given point in time.
Elasticity	Due to Distributed Nature and SOA of Cloud computing; Cloud Computing enables user as well as service providers to add/remove any user/resource to/from the cloud dynamically without affecting its working.
Automation	Build, deploy, configure, provision, and move, all resources without manual intervention
Metered billing	Per-usage business model; pay only for what one use

B. Security for the Cloud

What, if the cloud itself get attacked? Apart from good compartmentalization and integration of various cloud services, it is necessary that Cloud itself must be protected

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-46

from unauthorized use and access. Authentication of users and monitoring incoming and outgoing traffic plays very important role in this case. Cloud can use Antivirus, Antispammer, honeypots, Firewalls etc, to protect data from corruption. If by somehow the data get corrupted by viruses then in many cases data recovery becomes a nightmare; here data redundancy helps in recovery of data. Access of data to any untrusted party can compromise the whole purpose of cloud computing and thus a proper intrusion detection, demilitarized zones (DMZ), Honypots and like security mechanisms becomes a must part of any security in cloud computing objective [7, 10–12].

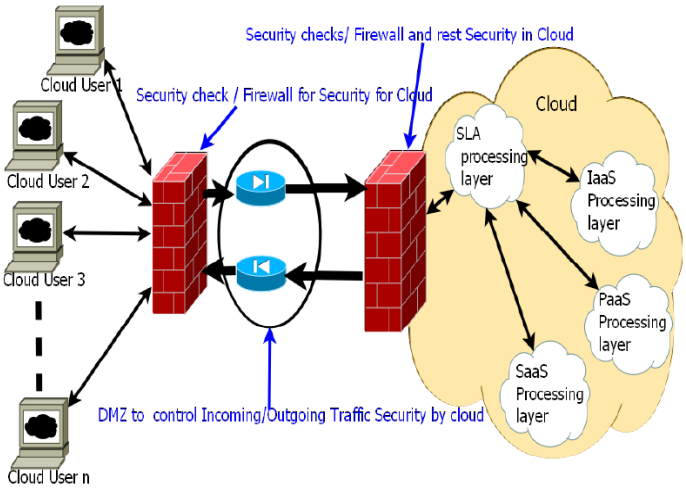

Figure 2. Three dimensional security requirement of cloud

DMZ, Firewalls, Multi level authentication(MLA) of users can help in protecting cloud from many breaches and attacks. In MLA user generally enter some predefined combinations of events and passwords from different media with username to get the authentication for data access and other operations in cloud. MLA with other security measures can help making cloud more secure [11, 13, 22].

Integration of cloud services and components plays important role in increased throughput of the cloud with providing security for it; and so maintaining proper integration of all resources, services and components of cloud is desirable. Every service must have to be checked for its integrity prior to its launch for user. Cloud computing involves heavy use of distributed and parallel processing with networking; this if not properly integrated can create problems in load balancing, process/resource migration, resource utilization etc… Proper integration of cloud services and components provides security for cloud by assuring a failure resistance [6].

C. Security by the Cloud

End user must have to get the secure access and privacy when he uses the cloud [13]. This issue won't get addressed properly if Issues IV-A and IV-B won't get implemented with utmost care. Security in cloud assures data availability through redundancy and data security through compartmentalization and data encryption and decryption. Security for cloud ensures traffic control, monitoring of data, integration of system, etc, making cloud secure from inside and from outside. User sees the integration of these two security aspects of cloud as security by cloud to her data or computations [6, 22].

Security by the cloud involves saving users data in such manner that even if the data is stolen by some one or if some one get an inadvertent access to users data, in both cases the data must not have to be easily interpretable. This requires advanced data encryption and distributed storage schemes to store the data. Implementing AES (Advanced Encryption Schemes) and like mechanisms to make users data unavailable to others, only can assure privacy and security. Use of proper key distribution algorithms for encrypting/decrypting the decrypted/encrypted data, providing protected access to data etc, are the few measures that can be employed here [10].

Security by cloud just not involves the technical security, it also offers legal security to the cloud user. This simply extends to taking legal actions against the person(s) responsible for any security breach that happened due to human error; eg. Sharing of users credential by cloud providers employee to third party or abuse of the same. Though this won't came as pure part of computer engineering and technology, SLA [8,15, 16, 21] need to provide for this by considering the international laws on copyrights, privacy, intellectual property rights and some criminal laws [20].

v. Common Security Threats & Remedial Measures

1) Abuse of Cloud Computing: By abusing the relative anonymity behind cloud registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. This problem is more general with public cloud. Inside employees of cloud provider can also take advantage of their access rights to steal/manipulate information in cloud. They can provide vital information of users/cloud to outsider for some personal reasons; or, may even damage the cloud operation using their positions. This threat is common to any system[6,22]. Following Precautions[10,11,22] should be taken to avoid/nullify the abuse.

a) A strict supply chain management with a comprehensive supplier assessment will leave a little room to employees for making any bad move. b) Legally bound human resource requirements as part of legal contracts will by fear of law restrain employees to some extent from abusing the system.

c)Transparent information security and management practices with periodic compliance reporting can be used to prevent any mishap from employees. d) A real time surveillance system to determine security breach and notifying of it instantly can restrain employee from abusing system. e) Implementation of stricter initial registration and validation processes like MLA can help. f) Implementation of enhanced credit card/net banking fraud monitoring and coordination to detect valid user and restrict inadvertent user is essential. g) Comprehensive

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-46

introspection of customers' incoming and outgoing network traffic is necessary. A multi check of traffic for data content (using DMZ, Firewalls, Antiviruses, AntiSpammers, Honeypots, etc), traffic nature (whether a good or Denial of Service attack), resource utilization (over utilization of resources by one user may starve others), is essential. h) Monitoring public blacklists for ones own network blocks. Public blacklists might be some sites/data with virus contents or some users with bad reputation. No access should be given to Public blacklists.

2) Insecure Interfaces or APIs: Cloud computing provider expose a set of software interfaces or APIs that users use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent Cloud-policy [6, 16].

A secure API can be designed by considering following designing and implementation measures. a) Minimize and nullify weaknesses in security model of cloud provider interfaces by exposing it to rigorous tests before deployment. b) Strong authentication and access controls are must in concern with encrypted transmission [13]. c) Create measures to understand and protect the dependency chain associated with the API.

3) Heterogeneity and Shared Technology Issue: This arises mainly in free public cloud. Heterogeneous resources used in building the infrastructure of cloud and their incompatibility with each other can slow down or even halt the cloud [12,22]. These resources may even not be made for multiuser architecture of the cloud. To address this gap, a virtualization hypervisor [18] mediates access between guest operating systems and the physical compute resources. A three aspect (in/for/by) security, with a)compute, storage, and network security enforcement and monitoring; b) Strong compartmentalization should be employed to ensure no inadvertent access of anything in cloud by any user. Users should not have access to any other tenants actual or residual data, network traffic, c) Strong encryption and decryption of data, making it non-readable if by some how unintended user get it.

4) Data Loss or Leakage: This threat increases in the cloud, due to architectural or operational characteristics of the cloud environment. Minimization of data loss or leakage [6, 22] can be achieved using a) implementation of strong API access control, b) by protecting integrity of data in transit using advanced encryption system, c) by analyzing data protection at both design and run time. d) By implementing strong key generation, storage and management, and destruction practices. e) By contractually demanding providers wipe persistent media before it is released into the pool. f) By contractually specifying state of the art provider backup and retention strategies.

5) Account/Service Hijacking: Cloud computing uses existing networks, like Internet; so, attack methods such as phishing, fraud, and exploitation of software vulnerabilities, reuse of Credentials and passwords can results in Account/service hijacking. If an attacker gains access to cloud-users credentials, they can eavesdrop on users activities and transactions, manipulate data, return falsified information, and redirect users clients to illegitimate sites. Users account or service instances may become a new base for the attacker; as, they may leverage the power of users reputation to launch subsequent attacks. Safeguards [6, 13, 22] required for account to save from hijacking are a) Implementation of no-sharing policy of account credentials between users and services. b) MLA implementation wherever necessary; mainly in transactions involving crucial data or money. c) Employment of proactive monitoring to detect unauthorized activity.

TABLE II
COMMON SECURITY THREATS OF NETWORKING/CLOUD

Threat	Description
Denial of Services	Attackers prevents the normal use of Network by flooding it with garbage communication.
Eavesdropping	Attackers passively monitors network communication for data and authentication credentials
Man in the middle	Attacker can use the data acquired using eavesdropping to pose himself as legitimate party bypassing the real one
Masquerading	Attacker can pose as authentic user to gain some privileges unauthentically
Message modification	Attacker can modify the messages acquired in eavesdropping and then retransmitting them by posing as authenticate user
Message replay	Attacker can retransmit the messages acquired in eavesdropping unnecessarily by posing as authenticate user
Traffic analysis	Attacker can passively monitors network communication for data and authentication credentials for identifying traffic pattern to decide his attacking strategies

6) Unknown Risks: Due to complexity of cloud computing many unknown risk situations may arise. To manage these risks a continuous monitoring and checks on the operation of cloud, and operatives inside and outside the organization using cloud is necessary [22]. Security measures/methods employed to handle the unknown risks may be the combination of few/all of the above. As cloud computing greatly relay on the networking, all the common security threats of networking listed in table II need to be addressed.

VI. Summary

Cloud computing is today's happening technology. Its various aspects need to be documented in sorted and clear manner so that new researchers/students of the technology can get every bit of information regarding its design and implementation. Security is one of the most important issue of design and implementation of any system. This paper discussed many of existing security issues and measures that

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-46

can be used to design and implement a cloud. Proper understanding of security is necessary to create a trusted and reliable system. The paper briefed out need for cloud security. Distinguished and discussed three aspects, in/for/by, of security; and discussed some common threats to security. Paper discussed in brief the points to consider while drafting

SLA; though SLA based security is practically difficult to implement.

References

[1] "US Government Driven Cloud Computing Standards A panel iscussion including: DMTF, Cloud Security Alliance, NIST and SNIA," Tech. Rep., 2011, pp. 1-45.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing (Draft)," National Institute of Standards and Technology, U.S. Department of commerce, Tech. Rep., 2011. [Online]. Available: www.nist.org

[3] "Cloud computing use cases," Tech. Rep., a white paper produced by the Cloud Computing Use Case Discussion Group. [Online] Available:http://groups.google.com/group/cloud-computing-use-cases

[4] S. Team, SECURED WSN-INTEGRATED CLOUD COMPUTING FOR U-LIFE CARE (SC3). Ubiquitous Computing Lab Kyung Hee University, 2009.

[5] B. Furht and A. Escalante, Eds., Handbook of Cloud Computing. Springer Science+Business Media, LLC 2010, 2010, iSBN 978-1-4419-6523-3, e-ISBN 978-1-4419-6524-0 DOI 10.1007/978-1-4419-6524-0, Springer New York Dordrecht Heidelberg London.

[6] R. L. Krutz and R. D. Vines, Cloud Security :A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing, Inc. 10475 Crosspoint Boulevard, Indianapolis, IN 46256, www.wiley.com , 2010, iSBN: 978-0-470-58987-8.

[7] A.S.Rumale and Dr.D.N.Chaudhari, "Cloud computing : Designing secure storage- cloud system," International Journal Of Computer Science And Applications, ISSN: 0974-1003, vol. 4, no. 3, pp. 120–124, Oct-Dec 2011.

[8] G. Jacobs, "Clearing the Sky in Cloud Computing: a Framework for SLA Elements in the Cloud. ," Series Master Theses Operations Management and Logistics, School of Industrial Engineering, Eindhoven University of Technology, February 2012.

[9] "Distributed computing: Utilities, grids & clouds," International Telecommunication Union : Telecommunication Standardization Policy Division ITU Telecommunication Standardization Sector, Tech. Rep., iTU-T Technology Watch Report-2009, pp.1-13.

[10] W. Jansen and T. Grance, Guidelines on Security and Privacy in Public Cloud Computing, ser. Draft Special Publication 800-144. Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, 2011, pp. 1-60.

[11] V. J. Winkler and B. Meine, Securing the Cloud : Cloud Computer Security Techniques and Tactics. Syngress is an imprint of Elsevier 225 Wyman Street, Waltham, MA 02451, USA, 2011, iSBN-978-1-59749-592-9, pp.1-315.

[12] D. M. I. Williams, "Risks of cloud computing," in A Quick Start Guide to Cloud Computing : Moving your business into the cloud , ser. New Tools for Business. Kogan Page Limited, 2010, pp. 39–55.

[13] S. Fox, D. Follette, G. Raja, and P. Stubbs, "Securing Cloud Solutions Using Claims-Based Authentication," in PROFESSIONAL SharePointR 2010 Cloud-Based Solutions. John Wiley & Sons, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256, 2011-12, pp. 309– 335.

[14] A. Rumale, "Synopsis on cloud computing : Designing secure channel application for storage-cloud system," As a partial fulfilment for consideration to Ph.D. Admission from the year 2011-12/2012-13 at Amravati University., July 2011-12, research Guide : Dr. D.N.Chaudhari.

[15] D. M. Dekker and D. G. Hogben, "Survey and analysis of security parameters in cloud SLAs across the European public sector ," European Network and Information Security Agency (ENISA), survey report, December 2011, pp. 1-36. [Online]. Available: http://www.enisa.europa.eu

[16] B. Ludwig and S. Coetzee, "Implications of security mechanisms and Service Level Agreements (SLAs) of Platform as a Service (PaaS) clouds for geoprocessing services," Applied Geomatics, Springer, pp. 1–13,2012.[Online].Available: http://dx.doi.org/10.1007/s12518G012G0083G3*

[17] P. Patel, A. Ranabahu, and A. Sheth, "Service level agreement in cloud computing," pp. 1–10, 2010-11.

[18] "Cloud Computing Security : Making Virtual Machines Cloud-Ready ," a Trend Micro White Paper May 2010, pp. 1-12.

[19] ASP-Team, Cloud Computing Certification Kit Specialist : Software as a service and Web Applications: The art of Service. The Art of Service Pty Ltd, 2011, pp. 1-219.

[20] A. Geyer, M. McLellan, Hunton, and Williams, "Strategies for Evaluating Cloud Computing Agreements," Bloomberg Finance, Bloomberg Law Reports Technology Law, 2011, pp. 1-4.

[21] N. R. Putri and M. C. Mganga, "Enhancing Information Security in Cloud Computing Services using SLA Based Metrics ," Master Thesis ,Computer Science , Thesis no: MCS-2011-03, School of Computing , Blekinge Institute of Technology , SE 371 79 Karlskrona, Sweden, January 2011.

[22] Cloud-Security-Alliance, "Top Threats to Cloud Computing V1.0," Cloud Secuirty Alliance, pp. pp. 1–14, Dec. 2010.

About Author (s):

Aniruddha S. Rumale, received his BE in Computer sci.& engg. in 1998 from Amravati University, and ME in CSE in 2008 from Pune University, and his MBA in HR from YCMOU, Nashik in 2012. At present he is pursuing Ph.D. in CSE(Cloud Computing) from Amravati University. He is working with SVPMs CoE, and has 14+ years of teaching experience with more than 40 papers authored in various National/International conferences & journals.

Dr. Dinesh N Chaudhari ,is working as Professor and Dean in computer engineering department of Jawaharlal Darda Institute of Engineering & Technology, Yavatmal. He is recognized Ph.D. guide at Amravati University and has more than 20 years of academic experience. His interests are in cloud computing, computer networking and security; and he has written many papers in national/international conferences and journals.