Safety Fear/Attacks Current in Cloud Environment

S MP Qubeb,
Assistant Professor,
CSE Department,
KG Reddy Engineering and Technology, Moinabad, Hyderabad.

Abstract : Cloud computing is a popular subject across the IT industry, but risks associated with this new technology and delivery model is not yet well understood. The biggest challenge in cloud computing is the security and privacy problems caused by its multi-tenancy nature and the outsourcing of infrastructure, sensitive data and critical applications. Enterprises are rapidly adopting cloud services for their businesses, measures need to be developed so that organizations can be assured of security in their businesses and can choose a suitable vendor for their computing needs. The boom in cloud computing has brought lots of security challenges for the consumers and service providers. How the end users of cloud computing know that their information i s not having any availability and security issues? In this paper we identify the most vulnerable security threats/attacks in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing and propose relevant solution directives to strengthen security in the Cloud environment. We also propose secure cloud architecture for organizations to strengthen the security

IndexTerms **- : Cloud Computing; Security and Privacy; Internet based Services, Secure Cloud Architecture**.

I. INTRODUCTION

With Cloud Computing becoming a popular term on the Information Technology (IT) market, security and accountability has become important issues to highlight. There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers.[1] In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.[2] Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure, training of personals or licensing new software [3].

NIST defines Cloud computing as a "model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and delivered with minimal managerial effort or service provider interaction" [4]. It follows a simple "pay as you go" model, which allows an organization to pay for only the service they use. It eliminates the need to maintain an in-house data center by migrating enterprise data to a remote location at the Cloud provider's site. Minimal investment, cost reduction, and rapid deployment are the main factors that drive industries to utilize Cloud services and allow them to focus on core business concerns and priorities rather than dealing with technical issues. According to [5], 91 % of the organizations in US and Europe agreed that reduction in cost is a major reason for them to migrate to Cloud environment.

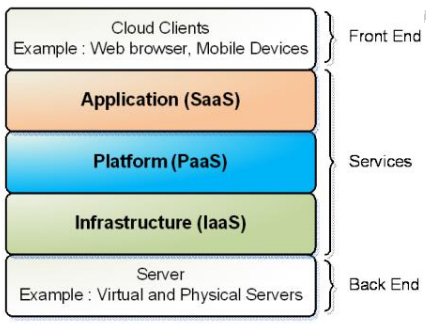

Figure 1: Cloud Computing represented as a stack of service

As shown in Figure. 1, Cloud services are offered in terms of Infrastructure-as-a- service (IaaS), Platform-as-a-service (PaaS), and Software-as-a-service (SaaS). It follows a bottom-up approach wherein at the infrastructure level; machine power is de- livered in terms of CPU consumption to memory allocation. On top of it, lies the layer that delivers an environment in terms of framework for application development, termed as PaaS. At the top level resides the application layer, delivering software outsourced through the Internet, eliminating the need for in-house maintenance of sophisticated software [6]. At the application layer, the end users can utilize software running at a remote site by Application Service Providers (ASPs). Here, customers need not buy and install costly software. They can pay for the usage and their concerns for maintenance are removed.

.

II. RELATED WORK

La'Quata Sumter et al. [7] says: The rise in the scope of cloud computing has brought fear about the Internet security and the threat of security in cloud computing is continuously increasing. Consumers of the cloud computing services have serious concerns about the availability of their data when required. Users have server concern about the security and access mechanism in cloud computing environment. To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the

movement and processing of the information kept on the cloud. They have identified there is need of security capture device on the cloud, which will definitely ensure users that their information is secure and safe from security threats and attacks. The proposed implementation is based on a case study and is implemented in a small cloud computing environment. They have claimed that there proposed security model for cloud computing is a practical model cloud computing. The advantage of their work is assurance of security to the end users of cloud. The limitation of this study is there proposed framework is not feasible for large scale cloud computing environments.

Meiko Jensen et al. [8] have shown that to improve cloud computing security, the security capabilities of both web browsers and web service frameworks, should be strengthened. This can best be done by integrating the latter into the former. M. Jensen et al. [9] focus on special type of Denial of Service attacks on network based service that relies on message flooding techniques, overloading the victims with invalid requests. They describe some well known and some rather new attacks and discuss commonalities and approaches for countermeasures. Armbust M Fox et al. [10] discuss that resources should be virtualized to hide the implementation of how they are multiplexed and shared.

Wayne [11]: In this paper benefits of cloud computing are highlighted along with the basic security issues that are still associated with cloud services. Shaping the security of critical systems is very important. Addressing the security issues faced by end users is extremely mandatory, Researchers and professionals must work on the security issues associated with cloud computing. Strong security policies must be designed to ensure data is safe and prevented from unauthorized access, in both corporate data centers and in the cloud servers. This research brings primary problems in terms of cloud security, which are alleged to cloud computing security and privacy issues.
Further the study gazes primary security and privacy Problems. It mainly focuses public clouds that needs significant consideration and presents required facts and figures to make organizations data security decisions. Key security issues identified and addressed in this paper are end user trust, Insider Access, Visibility, Risk Management, Client-Side Protection, Server-Side Protection, Access Control and Identity management. The strengths of their work is identification and discussion on cloud computing security issues which educates end users about security and private risks associated with cloud services. The weakness is that they haven‘t proposed any tool or framework to address identifies issues.

Rituik Dubey et al. [12] define different attacks scenarios and propose counter schemes for each. M. Okuhara et al. [13] explain how customers, despite their deep-seated concerns and uneasiness about cloud computing, can enjoy the benefits of the cloud without worry if cloud services providers use appropriate architectures for implementing security measures. They also describe the security problems that surround cloud computing and outline Fujitsu’s security architecture for solving them. [14] takes a detailed look at cloud computing security risks and conclude that, as computing takes a step forward to cloud computing, security should not move backward. Users should not accept moving backward in terms of security, and computing technology and security both, must advance together. [15] shows that some of the cutting edge technologies for cloud security are: self-protecting data, trusted monitors, and searchable encryption. With the integration of these technologies into their solutions, customers will have even more trust in their cloud provider. [16] discusses the fundamental trusted computing technologies on which latest approaches to cloud security are based.[17] argues that, with continued research advances in trusted computing and computation-supporting encryption, life in the cloud can be advantageous from a businessintelligence stand point, over the isolated alternative that is more common now- a- days. [18] describes Amazon Web Services’ (AWS) physical and operational security processes for network and infrastructure under Amazon Web Services (AWS) management. It also gives service specific security implementations for Amazon Web Services (AWS).

III. THREAT MODEL FOR CLOUD

An abstract view of threat model for Cloud computing is shown in Figure. 2. Cloud clients are facing two types of security threats viz; external and internal attacks.

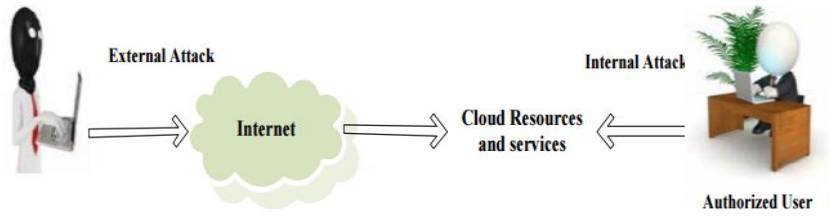

Figure 2: Threat model for Cloud computing.

External network attacks in the cloud are increasing at a notable rate. Malicious user outside the Cloud often performs DoS or DDoS attacks to a ffect the availability of Cloud services and resources. Port scanning, IP spoofing, DNS poisoning, phishing are also executed to gain access of Cloud resources. A malicious user can capture and analyze the data in the packets sent over this network by packet sniffing. IP spoofing occurs when a malicious user impersonates a legitimate users IP address where they could access information that they would not have been able to access otherwise. Availability is very important. Not having access to services when needed can be a disaster for anyone especially in the case of being denied service. This can occur when exhaustion of the host servers causes requests from legitimate consumers to be denied. This can cost a company large amounts of money and time if the services they depend on to operate are not available.
Internal attacker (authorized user) can easily get access to other user’s resources without being detected. An insider has higher privileges and knowledge (related to network, security mechanism and resources to attack) than the external attacker. Therefore, it is easy for an insider to penetrate an attack than external attackers.

IV. THREAT TO CLOUD COMPUTING

In this section, we discuss threats relevant to the security architecture of Cloud services. We discuss here some potential threats relevant to Cloud and their remedies based on our experience of implementing the cloud.[19].

Changes to business model: Cloud computing changes the way in which IT services are delivered. As servers, storage and applications are provided by off-site external service providers, organizations need to evaluate the risks associated with the loss of control over the infrastructure. This is one of the major threats which hinder the usage of Cloud computing services.

Mitigation: A reliable end-to-end encryption and appropriate trust management scheme can simplify such a threat to some extent.

Abusive use of Cloud computing: Cloud computing provides several utilities including bandwidth and storage capacities. Some vendors also give a predefined trial period to use their services. However, they do not have sufficient control over the attackers, malicious users or spammers that can take advantages of the trials. These can often allow an intruder to plant a malicious attack and prove to be a platform for serious attacks. Areas of concern include password and key cracking, etc. Such threats affect the IaaS and PaaS service models.

Mitigation: To remediate this, initial registration should be through proper validation/verification and through stronger authentication. In addition to this, the user's network traffic should be monitored comprehensively.

Insecure interfaces and API: Cloud providers often publish a set of APIs to allow their customers to design an interface for interacting with Cloud services. These interfaces often add a layer on top of the framework, which in turn would increase the complexity of Cloud. Such interfaces allow vulnerabilities (in the existing API) to move to the Cloud environment. Improper use of such interfaces would often pose threats such as clear-text authentication, transmission of content, improper authorizations, etc. Such type of threat may affect the IaaS, PaaS, and SaaS service models.

Mitigation: This can be avoided by using a proper security model for Cloud provider's interface and ensuring strong authentication and access control mechanism with encrypted transmission.

Malicious insiders: Most of the organizations hide their policies regarding the level of access to employees and their recruitment procedure for employees. However, using a higher level of access, an employee can gain access to confidential data and services. Due to lack of transparency in Cloud provider's process and procedure, insiders often have the privilege. Insider activities are often bypassed by a firewall or Intrusion Detection system (IDS) assuming it to be a legal activity. However, a trusted insider may turn into an adversary. In such a situation, insiders can cause a considerable effect on Cloud service offerings, for example, malicious insiders can access confidential data and gain control over the Cloud services with no risk of detection. This type of threat may be relevant to SaaS, PaaS, and IaaS.

Mitigation: To avoid this risk, more transparency is required in security and management process including compliance reporting and breach notification.

V. Shared technology issues/multi-tenancy nature: In multitenant architecture, virtualization is used to offer shared on demand services. The same application is shared among different users having access to the virtual machine. However, as highlighted earlier, vulnerabilities in a hypervisor allow a ma- licious user to gain access and control of the legitimate users' virtual machine. IaaS services are delivered using shared resources, which may not be designed to provide strong isolation for multi-tenant architectures. This may affect the overall architecture of Cloud by allowing one tenant to interfere in the other, and hence affecting its normal operation. This type of threat affects IaaS.

Mitigation: Implementation of SLA for patching, strong authentication, and access control to administrative tasks are some of the solutions to address this issue.

Data loss and leakage: Data may be compromised in many ways. This may include data compromise, dele- tion, or modification. Due to the dynamic and shared nature of the Cloud, such threat could prove to be a major issue leading to data theft. Examples of such threats are lack of authentication, authorization and audit control, weak encryption algorithms, weak keys, risk of association, unreliable data center, and lack of disaster recovery. This threat can applicable to SaaS, PaaS, and IaaS. Mitigation: Solutions include security of API, data integrity, secure storage for used keys, data backup, and retention policies

Service hijacking: Service hijacking may redirect the client to an illegitimate website. User accounts and service instances could in turn make a new base for attackers. Phishing attack, fraud, exploitation of software vulnerabilities, reused credentials, and passwords may pose service or account hijacking. This threat can affect IaaS, PaaS, and SaaS.

Mitigation: Some of the mitigation strategies to address this threat include security policies, strong authentication, and activity monitoring.

Risk profiling: Cloud offerings make organizations less involved with ownership and maintenance of hardware and software. This offers significant advantages. However, these makes them unaware of internal security procedures, security compliance, hardening, patching, auditing, and logging process and expose the organization to greater risk.

Mitigation: To avoid this Cloud provider should disclose partial infrastructure details, logs, and data. In addition to this, there should also be a monitoring and alerting system.

Identity theft: Identity theft is a form of fraud in which someone pretends to be someone else, to access resources or obtain credit and other benefits. The victim (of identity theft) can suffer adverse consequences and losses and held accountable for the perpetrator's actions. Relevant security risks include weak password recovery workflows, phishing attacks, key loggers, etc. This affects SaaS, PaaS, and IaaS.

Mitigation: The solution is to use strong authentication mechanisms.

.

V.ATTACKS ON CLOUD COMPUTING

By exploiting vulnerabilities in Cloud, an adversary can launch the following attacks.

Zombie attack: Through the Internet, an attacker tries to flood the victim by sending requests from innocent hosts in the network. These types of hosts are called zombies. In the Cloud, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. An attacker can flood the large number of requests via zombies. Such an attack interrupts the expected behavior of Cloud affecting availability of Cloud services. The Cloud may be overloaded to serve a number of requests, and hence exhausted, which can cause DoS (Denial of Service) or DDoS (distributed denial of service) to the servers. Cloud in the presence of attacker's flooded requests cannot serve valid user's requests.

Service injection attack: Cloud system is responsible for determining and eventually instantiating a free-to- use instance of the requested service. The address for accessing that new instance is to be communicated back to the requesting user. An adversary tries to inject a malicious service or new virtual machine into the Cloud system and can provide malicious service to users. Cloud malware affects the Cloud services by changing (or blocking) Cloud functionalities. Consider a case wherein an adversary creates his/her malicious services like SaaS, PaaS, or IaaS and adds it to the Cloud system. If an adversary succeeds to do this, then valid requests are redirected to the malicious services automatically.

Attacks on virtualization: There are mainly two types of attacks performed over virtualization: VM Escape and Rootkit in hypervisor.

VM Escape: In this type of attack, an attacker's program running in a VM breaks the isolation layer in order to run with the hypervisor's root privileges instead with the VM privileges. This allows an attacker to interact directly with the hypervisor. Therefore, VM Escape from the isolation is provided by the virtual layer. By VM Escape, an attacker gets access to the host OS and the other VMs running on the physical machine.

Rootkit in Hypervisor: VM-based rootkits initiate a hypervisor compromising the existing host OS to a VM. The new guest OS assumes that it is running as the host OS with the corresponding control over the resources, however, in reality this host does not exist. Hypervisor also creates a covert channel to execute unauthorized code into the system. This allows an attacker to control over any VM running on the host machine and to manipulate the activities on the system.

Man-in-the Middle attack: If secure socket layer (SSL) is not properly configured, then any attacker is able to access the data exchange between two parties. In Cloud, an attacker is able to access the data communication among data centers.

Metadata spoofing attack: In this type of attack, an adversary modifies or changes the service's Web Services Description Language (WSDL) file where descriptions about service instances are stored. If the adversary succeeds to interrupt service invocation code from WSDL file at delivering time, then this attack can be possible.

Phishing attack: Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. In Cloud, it may be possible that an attacker use the cloud service to host a phishing attack site to hijack accounts and services of other users in the Cloud.

Backdoor channel attack: It is a passive attack, which allows hackers to gain remote access to the compromised system. Using backdoor channels, hackers can be able to control victim's resources and can make it a zombie for attempting a DDoS attack. It can also be used to disclose the confidential data of the victim.

VI. SECURE CLOUD ARCHITECTURE FOR ENTERPRISE

As Shown in figure 3, we propose cloud security architecture, which protect organization against security threats and attacks. The key points for this architecture based on our analysis of existing security technologies are:

VI.I Single Sign-on (SSO)

Currently, Users are having multiple accounts in various Service Providers with different usernames accompanied by different password. Therefore the vast majority of network users tend to use the same password wherever possible, posing inherent security risks. The inconvenience of multiple authentications not only causes users to lose productivity, but also imposes more administrative overhead. Enterprises today are seriously considering the use of Single Sign On (SSO) technology [20] to address the password explosion because they promise to cut down multiple network and application passwords to one. To overcome this problem, it is suggested that, to streamline security management and to implement strong authentication within the cloud, organizations should implement Single Sign- On for cloud users. This enables user to access multiple applications and services in the cloud computing environment through a single login, thus enabling strong authentication at the user level.

VI.II Defense in depth Security Approach

As enterprise networking technology has evolved, so too has enterprise security. What began simply as setting up a perimeter around the network via fairly basic security tools like firewalls and email gateways, has evolved into adding an array of virtual private networks (VPNs), virtual local area network (VLAN) segmentation, authentication, and intrusion detection systems (IDS)—necessary to handle the consistently growing number of threats to the corporate network. Virtual firewall appliances should be deployed instead of first-generation firewalls. This allows network administrators to inspect all levels of traffic, which includes basic web browser traffic, to peer-to-peer applications traffic and encrypted web traffic in the SSL tunnel .Intrusion Prevention Systems (IPS) should be installed to protect networks from internal threats from insiders.

VI.III Increase Availability

Availability is a reoccurring and a growing concern in software intensive systems. Cloud systems services can be turned offline due to conservation, power outages or possible denial of service invasions. Fundamentally, its role is to determine the time that the system is up and running correctly; the length of time between failures and the length of time needed to resume operation after a failure. Availability needs to be analyzed through the use of presence information, forecasting usage patterns and dynamic resource scaling [21]. Access to cloud service should be available all the time, even during maintenance. This makes critical business data stored in the cloud to be always available to cloud users, reducing network down time, thereby increasing business profits. This can be done by implementing high availability technologies such as active/active clustering, dynamic server load balanced and ISP load balancing within the network infrastructure.

VI.IV Data Privacy

Cloud data privacy problem will be found at every stage of the life cycle. For the data storage and use, Mow bray et al. [22] proposed a client-based privacy management tool that provides a user-centric trust model to help users control their sensitive information during the cloud storage and use. Data loss prevention (DLP) tools can help control migration of data to the cloud and also find sensitive data leaked to the cloud. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network. DLP help a network administrator control what data end users can transfer.

VI.V Data Integrity

As a result of large scale data communication cost, the users don't want to download data but verify its correctness. Therefore, users need to retrieve the little cloud data through some kinds of agreements or knowledge's which are the probability of analytical tools with high confidence level to determine whether the remote data integrity. User can do the increase and decrease of the data capacity in the cloud server with the help of CSP(cloud service provider) in his request. This storage level must be with flexible and durability condition as far as its entire design or structure is concerned. Thus it should be claimed extra storage space concerning future process in data exchange.

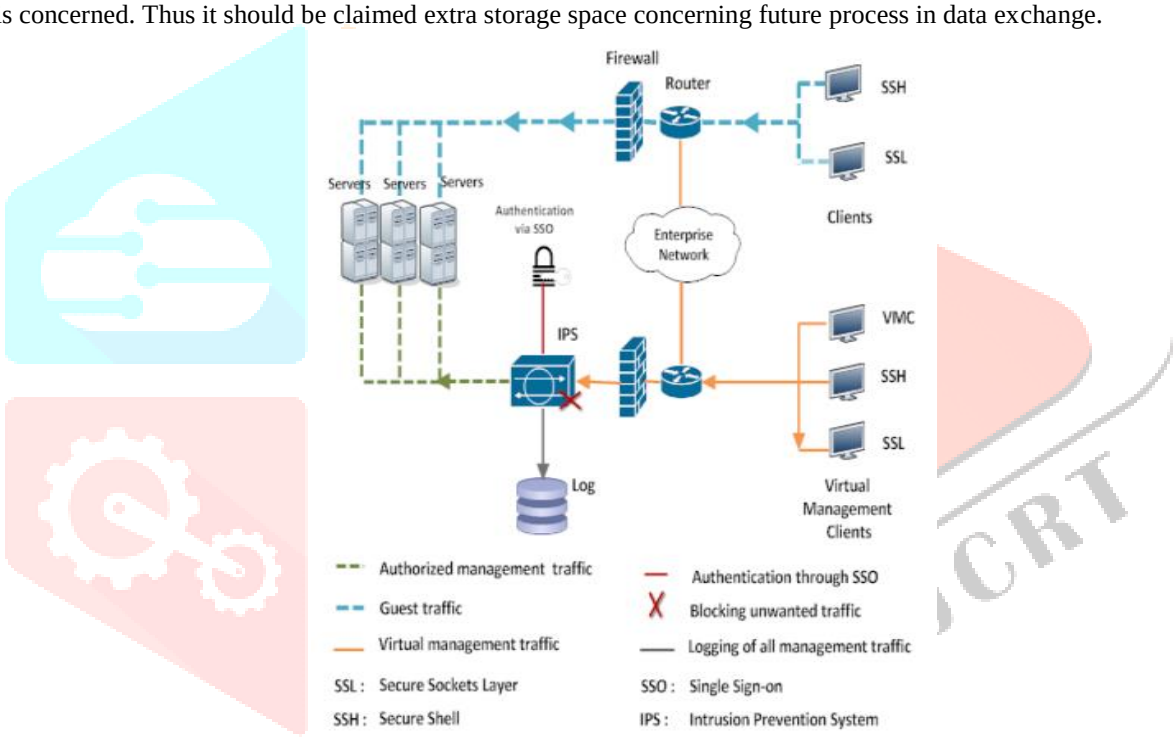

Figure 3: Secure Cloud Architecture

VI.VI Virtual Machine Protection

You can't just install your firewall or antivirus software on a cloud-based virtual machine. Physical firewalls aren't designed to inspect and filter the vast amount of traffic originating from a hypervisor running 10 virtualized servers. Because VMs can start, stop and move from hypervisor to hypervisor at the click of a button, whatever protection you've chosen has to handle these activities with ease. Plus, as the number of VMs increases in the data center, it becomes harder to account for, manage and protect them. And if unauthorized people gain access to the hypervisor, they can take advantage of the lack of controls and modify all the VMs housed there.

These virtual machines are vulnerable like their physical counterparts. Hence, to adequately protect virtual machines, they should he isolated from other network segments and deep inspection at the network level should be implemented to prevent them both from internal and external threats. Illegal internal access should be restricted by implementing intrusion prevention systems and unauthorized external access should be protected by using secure remote access technologies like IPSec or SSL VPN.

VII CONCLUSION

Organizations that are implementing cloud computing by expanding their on-premise infrastructure, should be aware of the security challenges faced by cloud computing. To protect against the compromise of the compliance integrity and security of their applications and data, defense in depth approach must be applied. This line of defense includes firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive organizations and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of their competitors. In this paper, a physical cloud computing security architecture has been presented. In future, the proposed architecture may be modified with the advancement of security technologies used for implementing this physical cloud security architecture.

REFERENCES

[1] "Swamp Computing" a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

[2] "Thunderclouds: Managing SOA-Cloud Risk", Philip Wik". Service Technology Magazine. 2011-10. Retrieved 2011- 21-21.

[3] What cloud computing really means. InfoWorld. http://www.infoworld.com/d/cloud-computing/what-cloudcomputing-really-means-031?page=0,0

[4] Mell P, Grance T (2011) The nist definition of cloud computing (draft). http://csrc.nist.gov/publications/drafts/800–145/Draft-SP- 800-145_cloud-definition.pdf

[5] Ponemon (2011) Security of cloud computing providers study. http://www.ca.com/~/media/Files/ IndustryResearch/security-of-cloud-computing-providersfinal-april-2011.pdf

[6] Software as a service-Wikipedia. Wikipedia. http://en.wikipedia.org/wiki/Software_as_a_service

[7] R. La'Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA

[8] Meiko Jensen ,Jorg Sehwenk et al., "On Technical Security,Issues icloud Computing "IEEE International conference on cloud Computing, 2009.

[9] M.Jensen ,N.Gruschka et al., "The impact of flooding Attacks on network based services"Proceedings of the IEEE International conference on Availiabilty,Reliability and Security (ARES) 2008.

[10] Armbrust ,M. ,Fox, A., Griffth, R., et al "Above the clouds: A Berkeley View of Cloud Computing" , UCB/EECS-2009- 28,EECS Department University of California Berkeley, 2009 http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS- 2009-28.pdf

[11] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciesnces 2011.

[12] Rituik Dubey et al., "Addressing Security issues in Cloud Computing"http://www.contrib.andrew.cmu.edu/~rdubey/in dex_files/cloud%20com puting.pdf

[13] M. Okuhara et al., "Security Architecture for Cloud Computing", www.fujitsu.com/downloads/MAG/vol46- 4/paper09.pdf

[14] "A Security Analysis of Cloud Computing" http://cloudcomputing.sys- con.com/node/1203943

[15] "Cloud Security Questions? Here are some answers"http://cloudcomputing.sys-con.com/node/1330353

[16] Cloud Computing and Security –A Natural Match, Trusted Computing Group(TCG) http://www.trustedcomputinggroup.org

[17] "Controlling Data in the Cloud:Outsourcing Computation without outsourcing Control http://www.parc.com/content/attachments/ControllingDataI nTheCloud- CCSW-09.pdf

[18] "Amazon Web services: Overview of Security processes " September 2008 http://aws.amazon.com

[19] Top 7 threats to cloud computing. HELP NET SECURITY. http://www.netsecurity.org/secworld.php?id=8943

[20] Rion Dutta, "Planning for Single SignOn", White Paper, MIEL e- Security Pvt

[21] M. Armbrust, et al., A view of cloud computing. Commun. ACM. vol. 53 (2010), pp. 50-58

[22] Miranda Mowbray and Siani Pearson, A client-based privacy manager for cloud computing. In Proc. Fourth International Conference on Communication System Software and Middleware (ComsWare), Dublin, Ireland, 16- 19 June 2009.