IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 4, Issue 5 (Sep-Oct. 2012), PP 11-18
www.iosrjournals.org

A Detailed Analysis of the Issues and Solutions for Securing Data in Cloud

Anindita Saha[1], Abhijit Das[2]
[1, 2](Department of IT, RCC Institute of Information Technology, India)

Abstract : *Cloud computing, the next generation architecture of IT enterprises, offers us with a flexible computing environment. In cloud, the virtualized resources are provided as a service over the internet. Typical applications that have already been thought of are SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) etc., which may provide common business applications online that is to be accessed from a web browser. Unlike traditional computing, the cloud moves the application software and databases to a set of networked resources. This enables the data to be accessed from anywhere and anybody simultaneously. Due to the fast growing markets of the cloud and also because of its unique nature, data security in cloud is an important concern. In order to secure the data in cloud, we have to ensure that the data is protected in every level during its flow and also during its storage. In this paper we identify and classify different threats to the data residing in a cloud and also provide separate solutions to these attacks. We also propose a multi-layered security architecture which can ensure the data security aspects and protect the data as it flows from browser to server level.*

Keywords: *cloud computing, data security, encryption, security attacks, security issues*

I. INTRODUCTION

Cloud computing is an emerging technology with a flexible computing environment which brings the concept of virtualized resources, on-demand services, pay as per use, online data storage and many more services over the internet. It has brought a significant change in the field of IT infrastructure by introducing the theme of virtualization and by reducing huge costs. The definition of cloud as given by NIST [1] is “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.” The five essential characteristics include On-demand service, Broad network access, Resource pooling (location pooling), Scalable & elastic and Metered services. The three service models are: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The four deployment models are: Private Cloud, Public Cloud, Hybrid Cloud and Community Cloud.

There are many advantages of cloud computing, for example, accessibility around the globe, reduced hardware and maintenance cost, agility, scaling, collaboration, flexibility and highly automated process where one need not worry about software up-gradation [2, 3]. Cloud computing improves the utilization of network resources many fold [4, 5]. It is different from other traditional computing in various aspects such as on-demand service, user centric interfaces, autonomous system [6], etc. With increasing popularity day by day, it is also facing the ever consistent challenge of security. One of the major concerns regarding cloud security is user’s data. The data can be accessed by user anytime and from anywhere in the world and is often subject to number of changes. Moreover the user never knows where the data is actually residing. This gives rise to a number of security threats from which the data needs to be protected. This paper analyses the known security issues and aims at suggesting a multi-layered security architecture which can protect the data in a cloud from sixteen security attacks which occur from browser to server level.

The rest of the paper is organized as follows: in section II, we talk about the services of the cloud. In section III, we describe the four deployment models of the cloud. In section IV, we talk about the security issues. In section V, we describe all attacks and their solutions and finally in section VI, we propose the multi-layered security architecture. Then, in section VII, we conclude by summarizing our paper.

II. THE SERVICE MODELS OF CLOUD

According to the different types of services offered, cloud computing can be considered to be consisting of following three layers:

- *Software as a Service (SaaS)* - It includes implementation of end user applications delivered on demand on a pay per use basis. The major benefit is that there is no compatibility issue and no licensing risk involved. The software requires no installation; instead one can get the service of the software directly from the cloud. It reduces the hardware cost as well. Moreover, the cloud allows the flexibility of using it anytime and from anywhere in the world. The user pays only as per his requirement and does not need to purchase the whole software. A few examples are Lotus Live from IBM, Gmail from Google and .NET service from Microsoft.

- *Platform as a Service (PaaS)* **-** PaaS provides software execution environment through platforms such as operating system. It enables software applications to be given a platform on which they can be executed with no requirement for administration of the lower level components. PaaS eliminates the hardware dependency and capacity concerns. It also provides a simplified deployment model. Examples are BlueCloud from IBM, Google App Engine from Google, Windows Azure from Microsoft and Force.com from Salesforce.com.
- *Infrastructure as a Service (IaaS)* **-** It supports various operations covering a wide range of features, from individual servers, to private networks, disk drives, various long term storage devices as well as email servers, domain name servers as well as messaging systems. All of these can be provisioned on demand and often include software license fees for operating systems and associated software installed on the servers. Organizations can build a complete computing infrastructure using IaaS on demand. Some examples of IaaS are Ensembles from IBM, Simple Storage Service and Elastic Compute Cloud from Amazon.

The IaaS model sits at the lowermost implementation layer, providing basic infrastructure support service and requires protection mainly at networking, trusted computing, and computer/storage levels. PaaS is the middle layer and demands protection at resource-management level including the protection required by IaaS. SaaS occupies the top most layer and features applications on data, content, and metadata using special Application Programming Interfaces (APIs) offered as service on demand [7]. It needs all protection functions at all levels.

III. THE DEPLOYMENT MODELS OF CLOUD

A. *Public Cloud*

A public cloud is owned by a cloud provider and made available to the general public on a multi-tenant, pay as per requirement basis. It is managed by a 3rd party [8]. Multiple enterprises can work on the infrastructure provided, at the same time.

B. *Private Cloud*

A private cloud is owned and deployed by an organization for internal use as a single tenant, and not typically pay as per requirement basis unless hosted by a 3rd party for dedicated use.

C. *Community Cloud*

A community cloud is co-operatively shared by a select set of tenants, often by organizations that are related by a common industry.

D. *Hybrid Cloud*

A hybrid cloud spans the cloud deployment models listed above, enabling applications and data to easily move from one cloud to the other.

IV. CONCERNS ABOUT CLOUD SECURITY

The security of data in a cloud is a major concern due to the dynamic nature of the cloud. The virtualized nature of the cloud makes the traditional methods unsuitable for the data security of cloud. This unique nature of cloud gives rise to some security issues which are discussed below. These issues need to be resolved in order to secure the data in a cloud.

A. *Abuse and nefarious use of cloud computing*

This issue arises whenever a cloud has very weak registration system. Many cloud providers give free usage for a certain period of time. This creates opportunity for malicious insiders to conduct their activities. PaaS providers have suffered a lot from these kinds of attacks and recently IaaS providers are also suffering from these attacks.

B. *Insecure Application Programming Interfaces*

The cloud users are provided with many softwares and Application Programming Interfaces (APIs) to interact with the cloud services. The security of cloud services is dependent on these APIs. The supervision of cloud is maintained using these APIs. Therefore weak interfaces and APIs may expose the cloud data to various security threats such as inflexible access control, limited monitoring, improper authorizations and many more malicious attempts. All the three services viz. SaaS, PaaS and IaaS can suffer from this issue.

C. *Malicious Insiders*

A malicious insider can cause innumerable security threats to a cloud service provider. Depending on the access granted, a malicious insider has the ability to harvest confidential data, cause financial loses, cause productivity losses to a organization and even monitor confidential activities and many more. All three SaaS, PaaS and Iaas can suffer from it.

D. Shared Technology Vulnerabilities

IaaS service providers deliver their services by sharing infrastructure. The infrastructure developed may not have strong separation properties to support a multitenant architecture. A virtualization hypervisor mediates access between guest operation system and physical compute resources which may allow the guest operating system to take an inappropriate control of the IaaS platform.

E. Loss of Governance

Certain issues may arise when the user give up the control to the cloud service provider. This may cause security threat as the user loses control over the data. The loss of control may account for lack of confidentiality, data integrity and availability.

F. Lock-In

Inability of the customer to move from one cloud service provider to another cloud service provider is called lock-in. A few tools are there for the portability but they are not sufficient and data leakage may occur during the process.

G. Data Loss or Leakage

The data present in cloud is subjected to a lot of security threats due to the unique nature of the cloud. Security of dynamic data is much harder since these data flows in cloud. There are innumerable ways of compromising data. Even loss of an encoding key may result in effective destruction of data.

H. Account, Service and Traffic Hijacking

It is a very old method and includes phishing, fraud, exploitation of software vulnerabilities etc. Reused passwords and credentials increase the probability of these attacks. If an attacker gains access to one’s credentials, then he can spy on the transactions, manipulate data and can even make it the base for subsequent attacks.

I. Unknown Risk Profile

Easy registration procedure in a cloud may create an opportunity for an attacker to make a fake profile and gain access to the cloud. This may result in loss of data confidentiality, availability and even destruction of data.

J. Management Interface Compromise

Cloud service providers give remote access to customers by using management interfaces which may pose a serious threat if web vulnerabilities are present.

K. Compliance Risks

The risk of legal or regulatory sanctions, financial loss, or loss to reputation a cloud service provider may suffer as a result of its failure to comply with all applicable laws, regulations, and codes of conduct and standards of good practice.

L. Browser Security

When a user sent request to the server by web browser, the web browser uses Secure Sockets Layer (SSL) to encrypt the credentials to authenticate the user. In this procedure, an attacker may get the credentials by decrypting the data and use these credentials as valid user. Thus the attacker gets access to the cloud and become capable of damaging the cloud activities in all possible ways.

V. SECURITY ATTACKS AND SOLUTIONS

After discussing the security issues, we will now talk about the probable attacks [9, 10, 11] which are responsible for these issues. We have distributed the attacks in four levels as shown below:

A. Browser Level

The security attacks which may occur in the browser level are:

1. Cookie Poisoning

Cookies may contain personal information of a user. By cookie poisoning, hackers can gain unauthorized information of a user using which the hacker is able to impersonate the real user. This allows him to gain all the access of the real user. Cookie Poisoning can be an effective tool for hackers because programmers store sensitive information in the supposedly invisible cookie.

Solutions

- Cookies can be protected by encryption [12]. Cookie encryption creates a digital signature that is used to validate the content in all future communications between the sender and the recipient. If the content is tampered with, the signature will no longer match the content and will be refused access by the server.

- Some Web Application Firewalls (WAF) can also block cookie poisoning attacks.
- Modern browsers allow the users to disable cookies. By default, Internet Explorer allows only third-party cookies that are accompanied by a P3P "CP" (Compact Policy) field [13]. Many browsers also allow a full wipe of private data including cookies. Add-on tools for managing cookie permissions also exist [14].

2. Hidden Field Manipulation

Certain fields are present in a web-page which are hidden and contain page-related information that is generally used by developers. These fields can be modified easily; hence they are highly prone to attack and may result in severe security breach [15].

Solutions

- Instead of using hidden form fields, the application designer can simply use one session token to reference properties stored in a server-side cache. When an application needs to check a user property, it checks the session cookie with its session table and points to the user's data variables in the cache / database.
- The name/value pairs of the hidden fields in a form can be concatenated together into a single string. A secret key that never appears in the form is also appended to the string. This string is called the Outgoing Form Message. An MD5 (Message Digest Algorithm) digest or other one-way hash is generated for the Outgoing Form Message. This is called the Outgoing Form Digest and it is added to the form as an additional hidden field. When the form is submitted, the incoming name/value pairs are again concatenated along with the secret key into an Incoming Form Message. An MD5 digest of the Incoming Form Message is computed. Then the Incoming Form Digest is compared to the Outgoing Form Digest (which is submitted along with the form) and if they do not match, then a hidden field has been altered.

3. SQL Injection Attack

SQL Injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.

Solutions

- *Parameterized Queries* - SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.
- *Validate Input* - The vast majority of SQL Injection checks can be prevented by properly validating user input for both type and format

4. Man In The Middle Attack (MITM)

This attack is quite popular to SaaS. As the name suggests, in this attack, a third party gains access when two parties are communicating with each other and SSL (Secure Socket Layer) is not properly configured. The intruder gets to know all data transferred between the two parties and can also inject false information between them.

Solutions

- This attack can be avoided by using encryption. Cain, Airjack, Ettercap, Dsniff etc are examples of some encryption technologies which can be used to prevent MITM attack. A detailed study preventing MITM attack is provided in [16].

5. Cloud Malware Injection Attack

In this attack, an attacker tries to inject malicious code which appears as one of the valid instances running on cloud. If successful, the cloud may suffer from eavesdropping. This can be achieved by slight modifications to change the functionality, or causing deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user. Here the attacker takes his first step by implementing his malicious service. This type of attack is also known as meta-data spoofing attack. When a user is set to run in the cloud server, the respective service accepts the instance for computation in the cloud. The only checking done is to establish if the instance matches a legitimate existing service. However, the reliability of the instance is not ensured. By breaking through the instance and replicating it as if it is a valid service, the malware activity succeeds in the cloud.

Solutions Utilization of the File Allocation Table (FAT) system architecture can be done since its straightforward technique is supported by virtually all existing operating systems. From the FAT table one can know about the code or application that a customer is going to run. This can be checked with the previous instances that had been already executed from the customer's machine and the validity and integrity of the new instance can be easily determined.

- Since cloud is totally OS (Operating System) platform independent, one can store the OS type of the customer and can cross check with the OS type from which the instance was requested.

B. Application Level

The security attacks which may occur in the application level are discussed below.

1. Hypervisor Issue

Cloud computing is based on the theme of virtualization. A hypervisor, also known as Virtual Machine Manager (VMM) is a virtualization technique which allows multiple operating systems known as "guest" operating systems to run simultaneously on a host computer. This feature is known as hardware virtualization. The hypervisor presents to the guest operating systems a virtual operating platform in such a way that the guest operating systems do not interfere with each other. Since multiple operating systems run on a single hardware platform, it becomes increasingly difficult to keep track of all as the number of operating systems increases. The security threats may arise in such a situation when a guest operating system tries to run a malicious code and brings the system down or takes control of the host operating systems and may also block access to other guest operating systems [17].

Solutions

- Different components of the hypervisor can be targeted [18] for various attacks. An advanced cloud protection system which monitors the activities of the guest VMs (Virtual Machines) and inter-communication among the various infrastructure components [19, 20] can be an effective tool.

2. Backdoor and Debug Options

It is a frequent practice of the developers to enable the debug options while publishing a website. These debug options, if left enabled unnoticed may provide an easy entry to an attacker into the website and let him make certain modifications at the web-site level [21].

Solutions

- Special attention must be given to backdoor and debug options that enable hackers to gain access and trespass into applications and these options must not be left unnoticed.

3. CAPTCHA Breaking

A CAPTCHA is a program that generates and grade tests in an attempt to ensure that the response is generated by humans. It is used to prevent spam and overexploitation of network resources by automated softwares. But recently, it has been found that CAPTCHA breaking is becoming possible by spammers [22]. An audio system may be provided for the visually- impaired users for reading CAPTCHA. The spammers use that audio system to read the CAPTCHA characters and use speech to text conversion to defeat the test.

Solutions

- Interaction with images can be a possible alternative for texting CAPTCHAs. Computer-based recognition algorithms require the extraction of color, texture, shape, or special point features, which cannot be correctly extracted after the designed distortions. However, humans can still recognize the original concept depicted in the images even with these distortions. A recent example of interacting with images CAPTCHA is to present the website visitor with a grid of random pictures and instruct the visitor to click on specific pictures to verify that they are not a robot (such as "Click on the pictures of the airplane, the boat and the clock").
- An easy equation can also be given and the user may be asked to give the answer to that equation. For example, (2*2+1=?).

4. Cross Site Scripting (XSS) Attack

XSS attack involves disguising a script as a URL variable within a URL from a legitimate site, and tricking a user into clicking on that URL. These may be hazardous links and when they are clicked, the script may get executed in the user's browser. XSS does not attack the website directly but it can be used to run arbitrary code in a user's browser and hack user's credentials.

Solutions

- Active Content Filtering, Content Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology etc are various techniques which have already been proposed [23] to overcome this attack.

C. Network Level

The threats which may arise in network level are:

1. DNS Attack

The translation of a domain name to an IP address is performed by DNS (Domain Name Server) server. In this attack, by calling the server by name, the user gets routed to some evil cloud which was not asked for.

Solutions

- DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats.

2. SNIFFER Attack

Capturing of packets of data flowing in a network is known as SNIFFER Attack. If the data is not encrypted, then the hacker gets to know the unencrypted data very easily which results in data leakage.

Solutions

- A sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network [28].
- The data should remain encrypted.

3. BGP Prefix Hijacking

It is a network attack where malicious intruder gets access to untraceable IP address when a wrong announcement related to IP addresses associated with Autonomous System (AS) is made. In certain cases a faulty AS can broadcast wrongly about the IP addresses causing the traffic getting routed to a different IP then the intended one. This causes data leakage.

Solutions

- An autonomous security system for autonomous systems has been explained in [29].

4. Port Scanning

Some security issues may arise regarding port scanning as Port 80(HTTP) is always open and is used for providing web services to user. Other ports may be opened only when needed. Therefore ports should be secured until and unless the server software is configured properly.

Solutions

- Ports should be secured by encryption.
- Firewall should be used to secure the data from port attacks.

D. Server Level

The security attacks which may arise in the server level are discussed below.

1. Denial of Service (DoS) Attack

A hacker can attack on the server by sending thousands of requests to the server due to which a server may become unresponsive to regular authorized users. This is known as DoS attack. This attack makes the data unavailable to the user during that time. This attack occurs when the number of requests that can be handled by a server exceeds its capacity. Besides causing congestion, DoS attack increases bandwidth consumption and make certain parts of the cloud unavailable.

Solutions

- The most popular method of protection against this attack is Intrusion Detection System (IDS) [24]. A defense association is used for resisting these types of attacks. Each cloud is loaded with separate IDS. The different systems work on the basis of information exchange. In case a specific cloud is under attack, then the co-operative IDS alert the whole system. In this way, this attack can be prevented.

2. Distributed Denial of Service (DDoS) Attack

A DDoS attack is an advance form of DoS attack. In this case also, the server is flooded by large number of requests send by the hacker so that the server becomes unresponsive to the legitimate users. The difference lies in the fact that the DDoS attack is relayed from different dynamic networks which have already been compromised unlike DOS. The hacker gets the full control of the flow of information. This attack has three units: Master, Slave and Victim. Master is the hacker who is causing the DDoS attack. The Slave is the network which provides the platform to launch this attack. Hence, it is also called coordinated attack. A DDoS attack is operational in two stages: the first one being Intrusion phase where the Master tries to compromise less important machines to support in flooding the more important one. The next one is installing DDoS tools and attacking the victim server or machine. Hence, a DDoS attack results in making the service unavailable to the authorized user similar to the way it is done in a DoS attack but different in the way it is launched.

Solutions

- The use of IDS in the virtual machine is proposed in [25] to protect the cloud from DDoS attacks.
- One can also have intrusion detection systems on all the physical machines which contain the user's virtual machines [26]. This scheme had been shown to perform reasonably well in a Eucalyptus [27] cloud.

3. XML (Extensible Markup Language) Signature Element Wrapping

A SOAP (Simple Object Access Protocol) message is generated in the server when a user requests from his VM through the browser. This message contains the structural information that will be exchanged between the browser and server during message passing. The XML document requires to be signed and the signature values should be appended before the message passing occurs. In this attack, the hacker does his trick during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message and the signature value both are duplicated. When the server checks the authentication, it cannot recognize this since the signature value is also duplicated. Thus, the attacker is able to intrude in the cloud and can run malicious code to interrupt cloud's normal functions.

Solutions

- This attack can be prevented by using the digital certificate e.g. X.509 authorized by third party such as certificate authorities. It uses the mixture of WS-security with XML signature to a particular component. XML should have the list of components so that it can reject the messages which have malicious file and also reject the unexpected messages from the client.

VI. THE MULTI-LAYERED SECURITY ARCHITECTURE

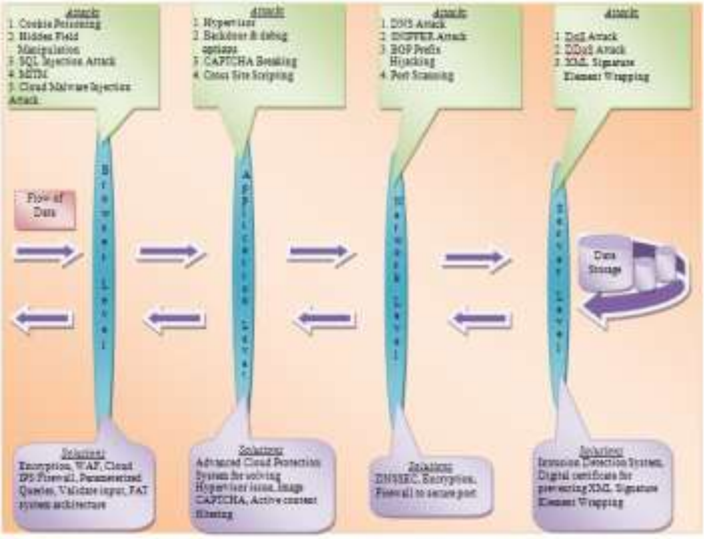
Attack:
1. Cookie Poisoning
2. Hidden Field Manipulation
3. SQL Injection Attack
4. MITM
5. Cloud Malware Injection Attack
Attack:
1. Hypervisor
2. Backdoor & debug options
3. CAPTCHA Breaking
4. Cross Site Scripting
Attack:
1. DNS Attack
2. DIGFTER Attack
3. BGP Prefix Hijacking
4. Port Scanning
Attack:
1. DoS Attack
2. DDoS Attack
3. XML Signature Element Wrapping
Flow of Data
Browser Level
Application Layer
Network Level
Server Level
Data Storage
Solutions:
Encryption, WAF, Cloud IPS Firewall, Parameterized Queries, Validate input, FAT system architecture
Solutions:
Advanced Cloud Protection System for solving Hypervisor issue, Image CAPTCHA, Active content filtering
Solutions:
DNSSEC, Encryption, Firewall to secure port
Solutions:
Intrusion Detection System, Digital certificate for preventing XML Signature Element Wrapping

Figure 1. The Multi-Layered Security Architecture for securing Cloud Data

Cloud is facing a lot of challenges due to its unique nature. We have already given solutions to the security attacks which may occur in cloud. It has been observed that the data which flows in cloud should be protected in every stage as it moves from browser to server and vice-versa. If a multi-layered architecture can be developed which can secure the data in every stage, then there is a possibility that the data shall stay secure. Hence, we propose a multi-layered architecture in figure 1 above, which can secure the cloud data. As the data moves, it should be secured from every attack in every level. In our architecture, we have shown the attacks which occur in the various stages and we have also proposed the solutions for these attacks. The data should also remain encrypted during its flow in cloud and also when it is stored in cloud to provide maximum immunity against data loss or leakage.

VII. CONCLUSION

Cloud computing has already revolutionized the world of IT and it is growing popular day by day. But it is not free from the ever growing challenge of security. Moreover, the traditional methods of ensuring security are not applicable for cloud. Therefore, ensuring security is a big challenge for cloud. In this paper, we have discussed many security issues which may occur in cloud. We have also given a detailed study of the security attacks which are responsible for these issues. The separate solutions to these attacks are also given. But there is a need of a compact architecture which will implement all these solutions. We have tried to give a theoretical approach to this thought and proposed the multi-layered security architecture which may be helpful in securing the cloud data.

VIII. Acknowledgements

We wish to give our heartiest gratitude to Dr. Kanchan Kumar Patra, Head of the Department of Science and Humanities, RCC Institute of Information Technology for his constant motivation, knowledge sharing and support behind this paper.

REFERENCES

[1] Peter Mell and Tim Grance, The NIST Definition of Cloud Computing, Version 15, 10-7-09, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf

[2] R. Maggiani, Communication Consultant, Solari Communication, Cloud Computing is Changing How we Communicate, *2009 IEEE International Professional Conference, IPCC,* pp. 1-4, Waikiki, HI, USA, July 19- 22, 2009. ISBN: 978-1-4244-4357-4.

[3] Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, Automated Control in Cloud Computing: Opportunities and Challenges, *Proc. of the 1st Workshop on Automated control for data centres and clouds*, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

[4] Sun Cloud Architecture Introduction White Paper. http://developers.sun.com.cn/blog/functionalca/resource/sun_353cloudcomputing_chinese.pdf

[5] Liupeng, Cloud computing [M].Beijing:Publishing House of Electronics Industry. 2011.1-10.

[6] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., Scientific Cloud Computing: Early Definition and Experience, *10th IEEE Int. Conference on High Performance Computing and Communications*, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[7] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, On technical Security Issues in Cloud Computing, *Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009),* pp. 109-116, India, 2009.

[8] R. L Grossman, The Case for Cloud Computing, *IT Professional, vol. 11(2),* pp. 23-27, 2009, ISSN: 1520-9202.

[9] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma, Cloud Computing Security – Trends and Research directions, 9780-7695-4461-8/11 $26.00 © 2011 IEEE

[10] Farzad Sabahi, Cloud Computing Security Threats and responses, 978-1-61284-486-2/111$26.00 ©2011 IEEE

[11] Yubo Tan , Xinlei Wang, Reasearch of Cloud Computing Data Security Technology, 978-1-4577-1415-3/12/$26.00 ©2012 IEEE

[12] D. Gollmann, Securing Web Applications, *Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK,* DOI:10.1016/j.istr.2008.02.002.

[13] 3rd-Party Cookies, DOM Storage and Privacy. grack.com: Matt Mastracci's blog. January 6, 2010. Retrieved 2010-09-20.

[14] How to Manage Cookies in Internet Explorer 6. Microsoft. December 18, 2007. Retrieved 2009-01-04.

[15] Ian Rathie, An Approach to Application Security, White Paper, SANS Institute. http://www.sans.org/reading_room/whitepapers/application/approach-application-security_16.

[16] Jonathan Katz, *Efficient Cryptographic Protocols Preventing Man in the Middle Attacks*, Doctoral Dissertation submitted at Columbia University, 2002, ISBN: 0-493-50927-5. http://www.cs.ucla.edu/~rafail/STUDENTS/katz-thesis.pdf /.

[17] Daniel Petri, What You Need to Know About Securing Your Virtual Network, Jan. 8, 2009. http://www.petri.co.il/what-you-need-to-know-about-vmware-virtualization-security.htm/.

[18] Berman, M., Virtualization Audit 101: The top 5 risks and recommendations for protecting your virtual IT, Computer Technology Review, Feb. 4, 2009.http://www.wwpi.com/.

[19] Flavio Lombardi, Roberto Di Pietro, Secure Virtualization for Cloud Computing, *Journal of Network and Computer Applications, vol. 34, issue 4*, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

[20] Hanqian Wu, Yi Ding, Winer, C., Li Yao, Network Security for Virtual Machines in Cloud Computing, *5th Int'l Conference on Computer Sciences and Convergence Information Technology*, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

[21] Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, Malicious Sniffing System Detection Platform, *Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04),* pp. 201-207, 2004, ISBN: 0-7695-2068-5.

[22] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, Intrusion detection techniques for Grid and Cloud Computing Environment, *IT Professional, IEEE Computer Society, vol. 12, issue 4*, pp. 38-43, 2010.

[23] Web 2.0/SaaS Security, Tokyo Research Laboratory, IBM Research. http://www.trl.ibm.com/projects/web20sec/web20sec_e.htm.

[24] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, Intrusion detection techniques for Grid and Cloud Computing Environment, *IT Professional, IEEE Computer Society, vol. 12, issue 4*, pp. 38-43, 2010.

[25] Aman Bakshi, Yogesh B. Dujodwala, Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine, *ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks,* pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[26] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, Integrating a Network IDS into an Open Source Cloud Computing Environment, *Sixth International Conference on Information Assurance and Security*, USA, pp. 265-270, Aug. 23-25, 2010. DOI: 10.1109/ISIAS.2010.5604069

[27] Eucalyptus web site, http:// www.eucalyptus.com/.

[28] Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, Malicious Sniffing System Detection Platform, *Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04)*, pp.201-207, 2004, ISBN: 0-7695-2068-5.

[29] Josh Karlin, Stephanie Forrest, Jennifer Rexford, Autonomous Security for Autonomous Systems, *Proc. Of Complex Computer and Communication Networks*; vol. 52, issue. 15, pp. 2908- 2923, Elsevier, NY, USA, 2008.