Levels of Security Issues in Cloud Computing

R. Charanya[1], M.Aramudhan[2], K. Mohan[3], S. Nithya[4]
[1,3,4] VIT University,Vellore -632014, India
1charanya.r@vit.ac.in
[2]PKIET, Karaikal, India

***Abstract*—Nowadays, Cloud computing is booming in most of the IT industry. Most of the organizations are moving to cloud computing due to various reasons. It provide elastic architecture accessible through internet and also it eliminate the setting up of high cost computing infrastructure for the IT based solutions and services. Cloud computing is pay-per-use model, on-demand network access to a shared pool of configurable computing resources like Application-as a service, Platform as a services and infrastructure as a services. In this paper, survey of security issues at different levels such as application level, host level and network level is presented.**

Keywords:- **Saas, Paas, Iaas, Application level, Network level, Host level**

I. INTRODUCTION

T Cloud computing is defined as provision of resources, application and information as a service over the cloud on demand. It supports the high storage capabilities and computational power. Today small and medium size companies are moving to Cloud due to various reason like reduced hardware, maintenance cost, pay-for-use, scalability, accessible location independent, on-demand security controls, fast deployment, flexibility and the highly automated process i.e. he customer need not worry about software up-gradation[22].

Cloud computing consist of three layers like Infrastructure as a service (Iaas) is a lowest layer, it provides the basic infrastructure support services, Platform as a service (Paas) is the middle layer providing environment for hosting user applications and Software as a service (Saas) is the topmost layer it provide the complete application is offered as a service on demand [6]. The user need not install and run the application in local computer, so it reduce the software maintenance burden.

I.1 Cloud Delivery Models

The Cloud computing services can be delivered to customer in many different ways. The cloud computing delivery models offering a various types of services like, Software as a service (SaaS), Platform as a service (PaaS) and infrastructure as a service (IaaS).

Infrastructure as a service:

It refers to sharing of hardware resources for executing services using virtualization technology. The resources will be scaled up based on demand. The charges will be based on pay-per use. The following resources are offered like hardware, data storage, networking and bandwidth.

Platform as a service:

It provides a higher-level software infrastructure where customers can build and deploy particular application and services using the tools and programming languages supported by the provider. Platform services are aimed at specific domains, such as the development of web applications, and are dependent on the programming language. Customers get a separated environment to test and develop or to permanently deploy their applications.It allows you to deploy applications without having to spend the money to buy the server **[13].**

Application as a service:

The customer can manage or control the underlying infrastructure and application platform. It refers complete application is hosted on internet, it eliminate the need to install in local computer and user can use them. Customers rent software hosted by the vendor. Popular software services are the Google Apps. It include web based email, calendar, contacts and chat appliances, Google Docs package allows access and sharing of documents, spreadsheets and presentations.

1.2 Cloud service deployment model is divided into four ways:-

1. Public cloud

Cloud infrastructure is hosted, operated and managed by a third party [20]. The infrastructure is available to all enterprise of all users. The service is offered to multiple customers over a common infrastructure. The services will be provided over the internet by the third party provider who shares the resources and pay what they used.

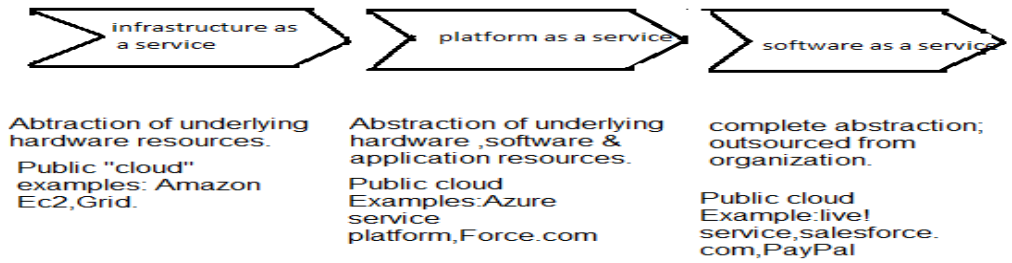

Fig 1. Delivery models

Service Models	Services	Example	Service Providers	Advantage
Saas (Consume)	Software is offered as Service and delivered through a browser	*Excel, WebPage, CRM, ERP* Access, SQL Server	*GoogleApps* *Salesforce.com*	*Reduce the cost* Centralized control
Paas (build on it)	Enables developers to write applications without installing any tools in local system but run on the cloud.	*Scripting* *Coding* Coding and integration	*AppEngine* *Azure* *Engine Yard* Force.com	*Scalability,* *Reliability and security* Pay-per-use
Iaas (Migrate to it)	Computing infrastructure is rented to the user	Infrastructure Scalability & Availability	*Amazon EC2,S3* *GoGrid* *Linode* Rackspace	*Scalability* *Pay as you go* Best-of-breed technology and resources

TABLE I Knowledge of delivery models

2. Private cloud

Cloud infrastructure is made available to specific customer and managed by organization or third party service provider [20]. Its good option to deal with data protection and service-level issues. Its owned by a single customer who controls which applications run, and where.

3. Hybrid cloud

Its a combination of public and private cloud models.

4. Community cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether its managed by them or third part service provider [2].

1.3 Five essential characteristic of cloud computing:-

On-demand self-service

Individuals can set themselves up without human interaction with a service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (mobile phones, Laptops and PDA).

Location independence Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically signed and reassigned according to consumer demand. Cloud computing is virtualized environment. The users can get the services at any place with any API. The demanded resources are from Cloud, is virtualized.

Rapid elasticity

It means users can rapidly increase and decrease

their computing resources as needed, as well as release.

Measured service

Users can pay for only the resources they actually use. Resource usage can be monitored, controlled and reported.

1.4. Advantage of cloud computing

Virtualization

Flexibility to choose vendor

Elasticity

Cost Reduction

II. OBSTACLES IN CLOUD COMPUTING

Many organizations are not yet confident to moving into the cloud .There are many security issues in cloud computing. The most important security issues must be avoided in order to make fully from this new computing paradigm. Some various security concerns are given and discussed here,

2.1. Data-Breach through Fibre Optic Networks

The major data-breach is data leaving a data-center to another data-center is a major security concern. The data transfer over a network of fibre-optic cables were considered to be a safe mode of data transfer, Telco Verizon's optical network is an illegal eavesdropping device is placed at a mutual fund company was discovered by US security forces[12].

2.2. Privacy and Security

The cloud service provider insists that data stored in server is protected from any of invasion and theft. Some company says that the data resides on the server is inherently more secure than residing in the personal computer [19].The security in cloud depends on the behaviour of these objects. It shares the multi-tenant environment, as the number of users increasing, security risk are also getting increased [18]. Its necessary to identify the proper security attacks protection mechanisms in client-side and also in server-side.

2.3. Portability and interoperability

Organizations are used to change the cloud providers, if they find another cloud platform better than the one they are using. Also some organizations use different cloud platforms to interact with each other to completing particular tasks [21]. The users have no idea where their information is stored [9]. User data stored in a shared environment, along with other user's data[3,5]. The inter-security handlings become important.

2.4. Data Storage over IP Networks

Now-a-days online data storage is very popular and majority of enterprise are stored the data in network. The main advantage is enterprise can store huge chunk of data without setting up required architecture. Disadvantage of having online storage, there are security threats that could cause data leakage or data unavailability in peak hours [17].

III. SECURITY PRINCIPLES

The fundamental basis for developing secure cloud environment is based on various security principles:

Confidentiality: The prevention of unauthorized disclosure of information that may be intentionally or unintentionally refers to the confidentiality.

Integrity: The concept of cloud information integrity is based on two principles Prevention of modification of data from unauthorized users and preventing the unauthorized modification of data by authorised user.

Availability: This Principle ensures the availability of cloud data and computing resources when needed**.**

Authentication: It refers to the process of testing the user's identity and ensures that users are who they claim to be.

Authorization: It refers to the privileges that are granted to individual or process for enabling them to access any authorized data and computing resources.

Accountability: This is related to the concept of non-repudiation where the person cannot deny from the

performance of an action. It determines the action and behaviour of single individual within cloud system.

IV. SECURITY CHALLENGES IN CLOUD COMPUTING

Before know about security management in cloud, it's necessary to analyse the various possible vulnerabilities and attacks in cloud environment. Top security threats in cloud computing is classified as network level, host level and application level.

4.1. Network level security issues

In public cloud architecture the data moves to or from the organization, ensure confidentiality and integrity. The network level security risk is classified as three types such as ensuring the data confidentiality, availability and integrity. The data and recourses previously confined to a private network are now exposed to the internet, share public network belonging to a third-party cloud provider. The user is not using HTTPS (but using HTTP) so it increase the risk. The types of network level security issues are

4.1.1. Eavesdropping

The unauthorized user access the data due to interception of network traffic, it result in failure of confidentiality. The Eavesdropper secretly listen the private conversation of others. This attack may done over email, instant messaging, etc,

4.1.2. Replay attack

Its a network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. The attacker intercepts and save the old messages and later it send to one of participants to gain access to unauthorized resources.

4.1.3. In Sybil attack

The malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user if malicious user is successful to compromise one of the honest user then attack gain unauthorized privileges that helps in attacking process.

4.1 4. Reused IP address

If user moves out of the network then same IP address is reassigned and reused by other customer, so it will create security risk to new user. A customer can't assume that network access to its resources is terminated upon release of its IP address. The old IP address is assigned to new user still the chance of accessing the data by some other user. The address still exists in the DNS cache, it violating the privacy of the original user. IP addresses are finite quantity and billable assert. There is a similar lag time between when physical (i.e., MAC) addresses are changed in ARP tables and when old ARP addresses are cleared from cache, an old address persists in ARP caches until they are cleared [1].

4.1.5. DNS Attacks

It translate the domain name to an IP address, Since domain name is easier to remember rather than IP address. The user using IP address in not feasible because has been routed to some other cloud instead of the one he asked. The sender and a receiver get rerouted through some evil connection. DNS security measures are taken, still the route selected between the sender and receiver cause security problems [7].

4.1.6. BGP Prefix Hijacking

It's a type of network attack in which wrong announcement on IP address associated with a autonomous system (AS), so malicious parties get access to the untraceable IP address.AS communicate using Border gateway protocol model. Faulty AS broadcast wrongly about the IP associated with it. In this case the actual traffic get routed to some other IP than the intended one [24]

4.1.7. Sniffer Attack

Data is flowing in network, and chance to read the vital information, it can be traced and captured. Sniffer program get recorded through the NIC (network Interface Card) that the data/traffic linked to other systems. Its easily detect a sniffing system running on a network is using ARP (Address resolution Protocol) and RTT (round Trip time) [16]

4.1.8. Port Scanning

If the customer configures the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. When Port scanning is detected it should be stopped and blocked.

4.1.9. Dos Attack

Dos attack is an attack it force the system component to limit, or even halt, normal services. The network is unavailable by flooding it , disrupting it, jamming it, or crashing it. The problem in Denial of service on the internet is impossible to prevent. DoS attacks can be prevented with a firewall but they have configured

properly.

4.1.1.10. Distributed Denial of Service Attack

Distributed Denial of Service attack is a DoS attack that occurs from more than one source, and from more than one location at the same time. DDoS attacks that comes from many "dummy" computers at the same time to flood the server. This is harder to trace or so that they can use more bandwidth.

4.2. Host Level Security issues:-

Cloud service provider do not publicly share information related to their host platforms, host operating systems, and processes that are in place to secure the hosts, since hackers can trying to intrude into the cloud service. The host level security issues are

4.2.1. Security concerns with the hypervisor

Hypervisor is defined as controller called as Virtual machine manager (VMM) that allows multiple OS runs on single machine at a time. If number of Operating system running on hardware platform, security issues get increased, because single hardware unit is difficult to monitor multiple operating systems. eg.:- guest system tries to run malicious code on the host system and get control of the system and block other guest OS, even it can make changes to any guest OS. Advanced cloud protection system can be developed, in order to monitor the guest VMs and inter communication among the various infrastructure components [10]

Virtualization platform is software. Major virtualization platform vendors are VMware, Xen and microsoft. Its important to secure the layer of software that sits between hardware and virtual servers. The isolation of customer VMs from each other in a multitenant environment, it is very important to protect the hypervisors from unauthorized users[21]. To protect the hypervisor the Iaas customer should understand the technology and security process controls instituted by the CSP.

4.2.2. Virtual server Security

Customers of Iaas have full access to the virtualized guest VMs that are hosted and isolated from each other by hypervisor technology. Virtual server may be accessible on the internet, so sufficient network access preventive steps should be taken to restrict access to virtual instances. The IaaS platform creates a risk due to self provisioning of new virtual server, that leads to create insecure virtual servers. Securing the virtual server in the cloud requires strong operational security procedures.

Some recommendations are

- Protect the integrity of the image from unauthorized users.
- Secure the private keys in the public cloud.
- Keep the decryption keys away from the cloud
- Do not allow password-based authentication for shell access.
- Require role-based access password
- Run a host firewall and open only the minimum ports necessary to support the services on an instance.
- Run only the required services and turn off the unused services
- Enable system auditing and event logging,
- Secure the log events to a dedicated log server.
- Keep the log server separate with higher security protection, including accessing controls.

4.3. Application level security threats:-

Some company hosts an applications in internet that many user use without considering about

Where, how, by whom the services are provided, so proper security mechanism should adapt. The types of

Application level security threats are

4.3.1. SQL Injection attack

Attackers inserted a malicious code into a standard SQL code and it allow unauthorized person to download the entire database or interact it in other illicit ways. The unauthorized user can access the sensitive data. This will be avoided the usage of dynamically generated SQL in the code.

4.3.2. Cross-site scripting [XSS]

It embedding script tags in URLs and when user clicks on them, the JavaScript get executed on machine. In dynamic websites, some pop ups windows get opened and request the user to click on that link, once user clicked the link the hacker get control and access all our private information [8].

4.3.3. EDoS

An attack against the billing model that underlies the cost of providing a service with the goal of

bankrupting the service itself. DoS attacks on pay-as-you-go cloud applications will result dramatic increase in your cloud utility bill, increased use of network bandwidth, CPU, and storage consumption. This type of attack is also being characterized as economic denial of sustainability (EDoS).

4.3.4. Cookie Poisoning

Cookies used to store User IDs. The two types of cookies are: persistent and non-persistent. Persistent cookie is stored on the client hard-drive, hacker who can access the client machine and easily access the cookies [15]. Non-Persistent cookie is stored in memory and more difficult to access. Another attack is unauthorized person can change or modify the content of cookies to access the application or web page. Cookies contain user identity credential information, one unauthorized person access these details then they can able to forge as an authorized user. This will be overcome by regular cookie cleanup.

4.3.5. Backdoor and debug options

Normally developers will enable the debugging option while publishing the web site. So hacker can easily enter into the web-site and make some changes [16]. To prevent this attack developer should disable the debugging option.

4.3.6. Hidden field manipulation

While user accessing the web page some fields are hidden and its used by developer. The hidden fields in HTML forms convey important information such as price, user ID etc. The attacker can save the catalogue page and change the value of hidden field and posted on web page. This will be severe security violation [14].

4.3.7. Google Hacking

Google search engine is the best option for the hacker to access the sensitive information. Even the hacker hack the user's account. Generally they try to find out the security loopholes on Google they wish to hack and then after having gathered the necessary information of the concerned system. A group of hackers in china hacks the login details of various g-mail users. The security threats can be launched at the application level and cause system downtime disabling the application access even to the authorized users.

4.3.8. Man in the middle attack

This attack is also a category of eavesdropping. The attacker set up the connection between two user and tries to hear the conversation or it provide false information between them. Tools like Dsniff, Cain, Ettercap, Wsniff, Airjack etc have developed to protect from this attack [25].

4.3.9. Dos Attack

Dos attack the services assigned to the authorized users unable to use by them. The attack, large number of services request handled by the server exceeds become unavailable to the authorized user. DoS attack increases bandwidth consumption besides causing congestion, Due to overloading of the server with the requests [14]. Making certain parts of the clouds inaccessible to the users.Intrusion detection system (IDS) is the most popular method of defense against this type of attacks[4].

4.3.10. Distributed Denial of services

DDos is advanced version of DoS in terms of denying the services running on a server is not able to handle it. Three functional units of DDos attacks: A Master, A Sleve and A Victim. Mater being the attack launcher is behind all these attacks causing DDoS, Slave is the network which acts like a launch pad for the Master. It provides the platform to the Master to launch the attack on the Victim. Hence it is also called as coordinated attack. The DDoS attack is operational in two stages: the first one being Intrusion phase and second one DDos tools. In intrusion phase the master tries to compromise the less important machines to support in flooding the more important one. The installing DDos tools and attacking the victim server or machine. DDos attack the services is unavailable to authorized user Its similar to Dos Attack but the way of launching is different. DDos attack was experienced with CNN news channel website is unable to access the site for a period of three hours [13].

Other Security Threats:

Failures in Providers Security

Security is necessary when designing cloud because cloud service provider controls the hardware and hypervisor on which data is stored and application also runs on the cloud infrastructure.

Attacks by other Customer

The cloud service provider resources shared with untrusted parties. The one customer can access the other customer sensitive information. This is highly possible in cloud. To overcome this problem strong cryptography, application-layer operation should be applied.

Availability and reliability issues

Cloud service is accessible through internet, so internet availability and reliability is essential. Service

accessible through internet so complexity increase due to change of failure. The countermeasures are monitoring the availability carefully.

Legal and Regulatory Issues

The cloud computing have many legal and regulatory issues regarding the data exposed outside the jurisdiction.

Perimeter security model broken

Many organizations use a perimeter security model with strong security at the perimeter of the enterprise network. Now all critical data and applications are stored in cloud but its outside the perimeter of enterprise control.

Integrated Provider and customer Security

The problem is disconnected provider and customer security systems. If there is any misbehaviour in cloud, not reported to the customer. The cloud service provider should adapt Proper integrity identity management.

Security problem	Attacks	Attack type	Preventive Method
Network Level	DNS attack	Sender and a receiver get rerouted through some evil connection.	Domain name system security Extensions (DNSSEC) reduces the effects of DNS threats.
	Eavesdropping	Attacker monitor network traffic in transit then interprets all unprotected data	Methods of preventing intruders are Internet protocol security(IP sec) Implement security policies and procedures install anti-virus software
	Dos Attack	Prevent the authorized user to accessing services on network	DoS attacks can be prevented with a firewall but they have configured properly Enforce strong password policies
	Distributed Denial of services	Attack against a single network from multiple computers or systems	Limit the number of ICMP and SYN packets on router interfaces. Filter private IP addresses using router access control lists.
	Sniffer Attack	Data is not encrypted & flowing in network, and chance to read the vital information.	Detect based on ARP and RTT. Implement Internet Protocol Security (IPSec) to encrypt network traffic System administrator can prevent this attack to be tight on security, i.e one time password or ticketing authentication
	Issues of reused IP addresses	IP address is reassigned and reused by other customer. The address still exists in the DNS cache, it violating the privacy of the original user	Old ARP addresses are cleared from cache
	BGP Prefix Hijacking	network attack in which wrong announcement on IP address associated with a autonomous system(AS), network attack in which wrong announcement on IP address associated with a autonomous system(AS)	Filtering and MD5/TTL protection(preventing the source of most attacks)
Host	**Security concerns with the**	Single hardware unit is difficult to monitor multiple operating systems. Malicious	Hooksafe that can provide generic protection against kernel-mode rootkits

Level	**hypervisor**	code get control of the system and block other guest OS.	
	Securing virtual server	Self-provisioning new virtual servers on an IaaS platform creates a risk that insecure virtual servers	Operational security procedures need to be followed
Application level	Cookie Poisoning	Unauthorized person can change or modify the content of cookies	Cookie should be avoided, or regular Cookie Cleanup is necessary.
	Backdoor and debug options	Debug options are left enabled unnoticed, it provide an easy entry to a hacker into the web-site and let him make changes at the web-site level	Scan the system periodically for SUID/SGID files Permissions and ownership of important files and directories periodically
	Hidden field manipulation	Certain fields are hidden in the web-site and it's used by the developers. Hacker can easily modify on the web page.	Avoid putting parameters into a query string
	Dos Attack	Services used by the authorized user unable to be used by them.	Intrusion Detection System (IDS) is the most popular method of defence against this type of attacks .Preventive tools are Firewalls,Switches,Routers,
	Distributed Denial of service attack	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.	Preventive tools are firewalls, Switches, Routers, Application front-end hardware, IPS based Prevention, etc.
	Google Hacking:-	Google search engine Best option for the hacker to access the sensitive information	Prevent sharing of any sensitive information Software solution such as Web Vulnerability Scanner
	SQL injection	Malicious code is inserted into a standard SQL code and gain unauthorized access to a database	Avoiding the usage of dynamically generated SQL in the code
	Cross site Scripting attacks	Inject the malicious scripts into web contents.	Various techniques to detect the security flaws like: Active Content Filtering, Content Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology

Table 2. Different types of attack and preventive method

V. CONCLUSION

Cloud computing is revolutionized the computing world, in order to keep the cloud secure, the security threats need to be controlled. Today, security is often listed as the number one concern for clients considering cloud adoption. This concern is immediately followed by high availability, a concept that needs to be addressed for almost every production-grade IT environment. So regularly auditing should be performed to safeguard the cloud from external threats. In this survey, security in cloud computing covers security issues and challenges in network level, host level and application level are identified and solution to prevent the attacks are compared.

Future work is to resolve the security issues in cloud using suitable framework.

REFERENCES

[1] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource allocation for security services in mobile cloud computing," in Proc. IEEE INFOCOM'11, Machine-to-Machine Communications and Networking (M2MCN), pp. 191-195, April 10-15, 2011, Shanghai, China.

[2] Rohit Bhadauria ,Rituparna Chaki,Nabendu Chaki and Sugata Sanyal, "A Survey on Security Issues in Cloud Computing,"2011 CoRR, VOL- abs/1109.538.

[3] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[4] 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.

[5] Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009. DOI: 10.1109/MIC.2009.103.

[6] 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.

[7] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve, "Cloud computing security: Routing and DNS security threats," http://searchsecurity.techtarget.com/tip/0, 289483, sid14_gci1359155_mem1, 00.html/.

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

[9] Eric Ogren, "Whitelists SaaS modify traditional security, tackle flaws," Sep. 17, 2009. http://searchsecurity.techtarget.com/news/column/0,294698,sid14_gci1368647,00.html/.

[10] 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/.

[11] John E. Dunn, "Spammers break Hotmail's CAPTCHA yet again", Tech-world, 16th Feb. 2009.http://news.techworld.com/security/110908/spammers-break-hotmails-captcha-yet-again/.

[12] Jessica T., "Connecting Data Centres over Public Networks," IPEXPO.ONLINE, April 20, 2011.http://online.ipexpo.co.uk/2011/04/20/connecting-data-centres-over-public-networks/.

[13] Nathan Mcfeters, "Recent CNN Distributed Denial of Service Attack Explained".http://www.zdnet.com/blog/security/recent-cnn-distributed-denial-of-service-ddos-attack-explained/1054.

[14] 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.

[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] 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.

[17] "Database Security in Virtualization and Cloud Computing Environment: The three key technology challenges in protecting sensitive data in modern IT architectures," Whitepaper, McAfee. https://portal.mcafee.com/downloads/General20Documents/database_security_in_virtualization_and_cloud_computing_environments.pdf.

[18] Jon Marler, "Securing the Cloud: Addressing Cloud Computing Security Concerns with Private Cloud," Rackspace Knowledge Centre, March 27, 2011, Article Id: 1638. http://www.rackspace.com/knowledge_center/private-cloud/securing-the-cloud-addressing-cloud- computing-security-concerns-with-private-cloud.

[19] George V. Hulme, "NIST formalizes cloud computing definition, issues security and privacy guidance",2011 http://www.csoonline.com/article/661620/nist-formalizes-cloud-computing-definition-issues-security-and-privacy-guidance.

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

[21] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning. Managing security of virtual machine images in a cloud environment. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96. November 2009.

[22] Miranda Mowbray, Siani Pearson. A Client-Based Privacy Manager for Cloud Computing. COMSWARE '09: Proceedings of the Fourth International ICST Conference on COMmunication System software and middleware . June 2009

[23] Flavio Lombardi, Roberto Di Pietro. Transparent Security for Cloud. *SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing*, pages 414-415. March 2010.

[24] 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.

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