International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 4– No.1, September 2012 – www.ijais.org

Taxonomy of the Security Aspects of Cloud Computing Systems-A Survey

Seyyed Mohsen Hashemi
Software Engineering and Artificial Intelligence Science and Research Branch, Islamic Azad University,Tehran, IRAN

Mohammad Reza Mollahoseini Ardakani
Dean of the Computer Engineering Department, Maybod Branch, Islamic Azad University, Yazd, IRAN

ABSTRACT

Cloud Computing is a model of both service delivery and consumption for increasing the capabilities of enterprises dynamically without investing in new infrastructure, training new personnel, or licensing new software. It refers to *everything* delivered as services over the Internet. Although the benefits of Cloud Computing are evident, security is one of the major issues which hamper the growth of cloud. In this paper, to facilitate identifying the security threats of cloud computing, we Taxonomy the security aspects of cloud computing systems and summarize the main security threats of it. Our taxonomy covers the four domains of cloud computing systems: infrastructure layer, platform layer, application layer and administration.

Keywords

Cloud computing security, Threats, Taxonomy

1. INTRODUCTION

In the past few years the concept of *cloud computing* has emerged as a viable and promising solution to the challenges associated with shrinking IT budgets and escalating IT needs. NIST, under the U.S. Department of Commerce, defines and describes cloud computing as "a model for enabling ubiquitous, 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"([2]). The cloud computing definition of NIST includes five essential features, three service models and four deployment models as figure 1 shown. Herein, the five essential features includes virtualized computing resource pool, broad network access, rapid elasticity, on-demand self-service, measured service; the three service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a service (SaaS); the four deployment models are private cloud, community cloud, public cloud and hybrid cloud. It is essential to understand that the service models, deployment models and the five characteristics of cloud computing as described by NIST do not run independently but are necessarily interrelated and connected to each other. Jerry Bishop, the Chief Information Officer at Chippewa Valley Technical College in Wisconsin, created a visual (see Figure 2) that displays these inter-relationships and necessary connections of the NIST cloud computing characteristics and models [3].

"The cloud offers several benefits (see Figure 3) like fast deployment, pay-for- use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services"([1]). While the cloud offers these advantages, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing. "According to a recent IDCI survey, 74% of IT executives and CIO's cited security as the top challenge preventing their adoption of the cloud services model (Clavister, 2009). Analysts'estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12% of the worldwide software market will move to the cloud in that period" ([1]).

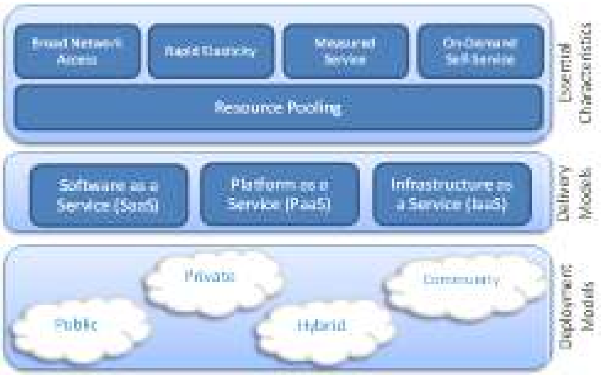

Fig 1: Visual Model of NIST Working Definition of Cloud Computing

2. SECURITY THREATS

The structure of the taxonomy used here (see table 1) is based on the service model layers of cloud computing plus administration factor (see figure 4). Of course, we do not claim that this classification and threats embedded in each category, is flawless and perfect. Particularly, many of these threats in different classes are overlapping. Here we mention some of the more exotic threats in each class.

2.1 Infrastructure layer threats

2.1.1Virtualization

Communication blind spot: "Virtualization introduces new challenges for enterprises to monitor and secure virtual networks. One of these challenges is named communication blind spot, because virtual machine-to-virtual machine (VM2VM) communications inside a physical server cannot be monitored by traditional network and security devices, this lack of visibility complicates problem identification and resolution" ([9]).

*Inter-VM Attacks and Hypervisor Compromises (VM Hopping): "*Virtualized servers use the same operating systems, enterprise applications, and web applications as physical servers. Hence, the ability of an attacker to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized environments as well” ([9]).

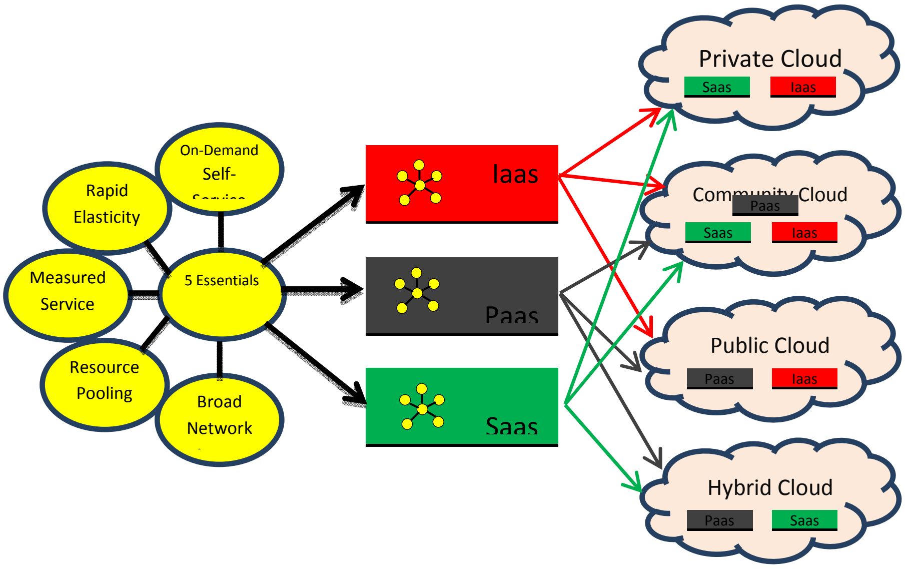

Fig 2: Interrelationships with Characteristics, Service Models and Deployment Models

“Once an attacker compromises one element of a virtual environment, other elements may also be compromised if virtualization-aware security is not implemented. In one scenario, an attacker can compromise one guest VM, which can then pass the infection to other guest VMs on the same host. Co-location of multiple VMs increases the attack surface and risk of VM-to-VM compromise. A firewall and an intrusion detection and prevention system need to be able to detect malicious activity at the VM level, regardless of the location of the VM within the virtualized environment. Another attack mode involves the hypervisor, which is the software that enables multiple VMs to run within a single computer. While central to all virtualization methods, hypervisors bring both new capabilities and computing risks. A hypervisor can control all aspects of all VMs that run on the hardware, so it is a natural security target. Therefore, securing a hypervisor is vital, yet more complex than it seems. Once an attacker can penetrates hypervisor, then he attacks other guest VMs on that host”([9]).

Mixed Trust Level VMs:“VMs with mission-critical data may reside on the same host as VMs with less critical data – resulting in mixed trust level VMs. Enterprises can attempt to segregate these different levels of secure information on separate host machines, but in some cases, this can defeat the purpose of a virtualized environment – to make the most efficient use of resources. Enterprises need to ensure that mission-critical information is protected while still realizing the benefits of virtualization. With self-defending VM security, VMs can remain safe even in mixed trust level environments, with protection such as intrusion detection and prevention, a firewall, integrity monitoring, log inspection, and antivirus capabilities”([9]).

Instant-On Gaps:“Beyond server consolidation, enterprises take advantage of the dynamic nature of VMs by quickly provisioning, cloning, migrating, and decommissioning VMs as needed, for test environments, scheduled maintenance, disaster recovery, and to support “task workers” who need computational resources on-demand. As a result, when virtual machines are activated and inactivated in rapid cycles, it is impossible to rapidly and consistently provision security to those virtual machines and keep them up to date. Dormant virtual machines can eventually deviate so far from the baseline that simply powering them on introduces massive security vulnerabilities. And new virtual machines, even when built from a template that includes security, cannot immediately protect the guest without configuration of the agent and conducting security updates. In short, if a guest virtual machine is not online during the deployment or updating of security software, it will lie dormant in an unprotected state and be instantly vulnerable when it does come online”([9]).

Resource Contention:“ Resource-intensive operations such as regular security scans and pattern file updates can quickly result in an extreme load on the system. When antivirus scans or scheduled updates simultaneously kick into action on all virtual machines on a single physical system, the result is an *antivirusstorm*. Similar storms can occur with other types of security scans and updates as well. These storms are like a run on the *bank*, where the bank is the underlying virtualized resource pool of memory, storage, and CPU. Server applications and virtual desktop environments are hampered by this performance impact. The traditional agent-based architecture also results in linear growth of memory allocation as the number of virtual machines on a single host grows. In physical environments, security software must be installed on each operating system. Applying this architecture to virtual systems means that each virtual machine requires additional significant memory footprint—an unwanted drain on server consolidation efforts”([9]).

VM Denial of Service:“DoS attacks are a threat to all servers, however an improperly configured hypervisor can allow a single VM to consume all resources, thus starving any other VM running on the same physical machine. DoS attacks make network hosts unable to function since critical processes do not have the hardware resources to execute in a timely manner” ([12]

Table 1. Taxonomy of the security aspects of cloud computing systems

Infrastructure	
Physical security	**Description**: The physical security of cloud computing systems encompasses the facilities and building services in which cloud computing systems are located or of which they are a part. **Threats**: ▪ Unauthorized access to the building ▪ inappropriate location and structure of datacenters ▪ Hardware failures(computer power supplies, cooling systems, …) ▪ Hardware interruption ▪ Hardware theft ▪ Hardware modification ▪ Misuse of infrastructure ▪ natural disasters
Virtualization	**Description**: Virtualization is mainly used in cloud computing systems to isolate user environments. At present virtualization is mainly used in datacenters to consolidate computers and to increase the use of the datacenter's capacity. **Threats**: ▪ Incorrect definition of Access rights to virtual machines ▪ migration of virtual machines between hosts ▪ communication blind spots ▪ Inter-VM Attacks and Hypervisor Compromises (VM Hopping) ▪ Mixed Trust Level VMs ▪ Instant-On Gaps ▪ Resource Contention ▪ VM Denial of Service (DoS) ▪ Malicious Insiders ▪ side channel attacks ▪ Session Hijacking
Host	**Description**: The host provides the environment in which the processes and their calculations are carried out. **Threats**: ▪ Unauthorized access to the processed data on the host ▪ the availability of the host ▪ Reliability of the calculations carried out on the host. ▪ DDoS attacks ▪ Shared Technology Issues ▪ Malicious Insiders ▪ Abuse and Nefarious Use of Cloud computing

continues

Network	**Description**: The network – and its components such as communication protocols and filter technologies – is another important part of the infrastructure which may influence the security of the cloud computing system. **Threats**: ▪ Connection flooding ▪ Disrupting communications ▪ DDoS attacks ▪ Traffic flow analysis ▪ Other traditional network attacks

Application	
Datasecurity	**Description**: Data security refers to the security of all data – including any existing configuration and meta data – which is stored and processed in cloud computing systems and transported between cloud computing systems and their services. The focus is on the protection goals of confidentiality and integrity in particular. **Threats**: ▪ Malicious Insiders ▪ Data Loss or Leakage ▪ Interception ▪ Privacy breach ▪ Modification of data at rest and in transit ▪ Data interruption (deletion) ▪ Exposure in network ▪ Uncontrolled super user rights that have the right to carry out the management and maintenance of data
Applicationsecurity	**Description**: Application security includes methods and procedures for ensuring authenticated access to cloud services and consideration of security criteria in the development of cloud services **Threats**: ▪ Insecure Interfaces and APIs ▪ Service Hijacking ▪ Session Hijacking ▪ malicious configuration changes ▪ Exceptions in cloud services ▪ malware infections ▪ media discontinuities when data is processed by the application ▪ impersonation of cloud users ▪ Traffic flow analysis ▪ Malicious Insiders ▪ “starvation” of an application ▪ And the most important threats to web applications

Platform	
Platformsecurity	**Description**: Platform security is mainly of interest to developers of cloud services who use a cloud platform such as Microsoft Azure, Google App Engine or Force.com to develop their own cloud applications. **Threats**: ▪ side channel attacks ▪ Abuse and Nefarious Use of Cloud computing ▪ Programming flaws ▪ Malicious Insiders

Administration	
Provider	**Description**: The administration of cloud services presents one of the main challenges from a security perspective. This is still given too little support by neither cloud vendors, nor are tools available to cloud users – or they are still in the process of being developed – which would enable them to manage their rented cloud services in an integrated and efficient manner. **Threats**: ▪ Unknown Risk Profile ▪ Poor identity and rights management ▪ Breach of contractual negotiations ▪ Malicious Insiders
Government	**Description**: Governments will play a vital role in different features of cloud computing e.g. securely managing the numerous and various scale cloud service providers, evaluating and ranking the security level of cloud service providers and the security credit of cloud customers, and publishing the proactive alarm of malicious programs, etc. **Threats**: ▪ sanction due to Political problems

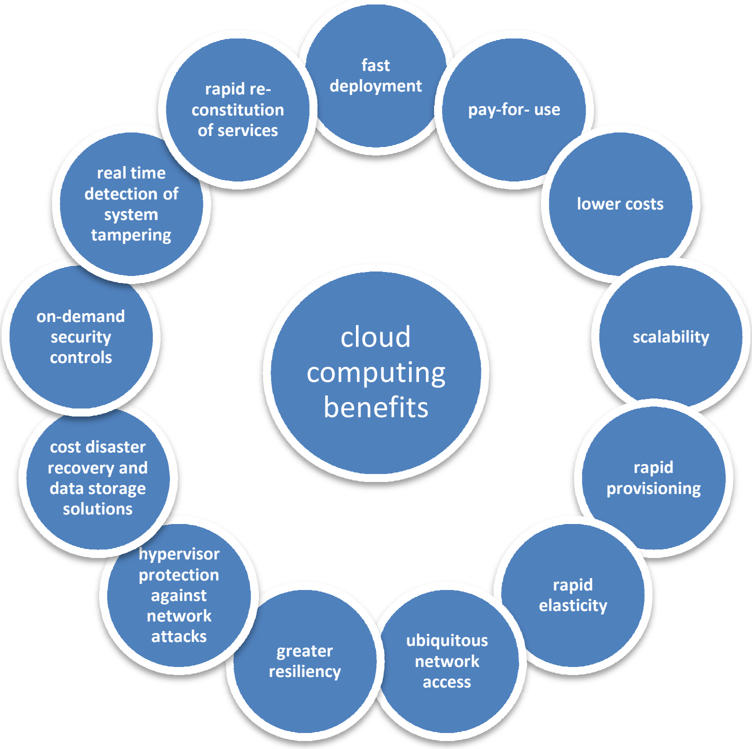
cloud computing benefits
fast deployment
pay-for- use
lower costs
scalability
rapid provisioning
rapid elasticity
ubiquitous network access
greater resiliency
hypervisor protection against network attacks
cost disaster recovery and data storage solutions
on-demand security controls
real time detection of system tampering
rapid re-constitution of services

Fig 3: Cloud Computing Benefits

2.1.2 Host

DDoS attacks: A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Shared Technology Issues:"IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To address this gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc."([5]).

Abuse and Nefarious Use of Cloud computing:"IaaS providers offer their customers the illusion of unlimited compute, network, and storage capacity - often coupled with a 'frictionless' registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some providers even offer free limited trial periods. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well. Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms" ([5]).

2.1.3 Network

Connection flooding:"Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic. Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests. By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host's memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service" ([13]).

Traffic flow analysis: flow is a unidirectional series of IP packets of a given protocol travelling between a source and a destination IP/port pair within a certain period of time. Different levels of analysis can be possible on this flow. So, Traffic analysis can be used by an attacker to detect network traffic anomaly.

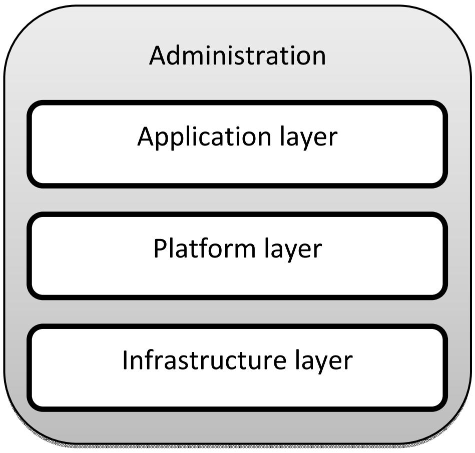

Fig 4: Taxonomy of the security aspects of cloud computing systems

2.2 Application layer threats

2.2.1 Data Security

Malicious Insiders:"Insiders" are not just employees and staff, but also service providers, business partners, consultants, contractors - any number of parties who may work for companies we deal with. “The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance” ([5]).

“To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection”([5]).

Data Loss or Leakage:“There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data. The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment”([5]).

2.2.2 Application Security

Insecure Interfaces and APIs:“Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency”([5]).

Service hijacking:“Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks” ([5]).

“Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks”([5]).

Session hijacking: “Session hijacking is a method of taking over a Web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network” ([14])

2.3 Platform layer threats

Side channel attacks:“In cryptography, a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Some side-channel attacks require technical knowledge of the internal operation of the system on which the cryptography is implemented, although others such as differential power analysis are effective as black-box attacks. The most powerful side channel attacks are based on statistical methods pioneered by Paul Kocher"([11]).

2.4 Administration Threats

2.4.1 Provider

Unknown Risk Profile:"One of the tenets of cloud computing is a reduction in hardware and software ownership and the associated maintenance. There is a danger, however, that in handing over ownership, responsibility for ensuring security procedures, policies and controls are followed may lapse - out of sight, out of mind. This can result in unknown exposures, particularly over time"([5]).

3. CONCLUSION

As described in this paper, though there are extreme benefits in using a cloud based system, there are yet many potential threats which must be dealt with. We believe that a first good starting point for improving Cloud Computing security is accurate identification of its threats. Thus, in this paper, we presented a range of potential threats to four domains of cloud computing systems: infrastructure layer, platform layer, application layer and administration.

4. REFERENCES

[1] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, pp. 1-11, 2011.

[2] P.Mell, T.Grance, (2011). "The NIST definition of cloud computing". National Institute of Standards and Technology, U.S. Department of Commerce. (Special Publication 800-145). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] J. Bishop, (2011). "Cloud definition model". Personal blog. Retrieved from http://blog.thehigheredcio.com/2011/02/23/cloud-definition-model/

[4] DimitriosZissis, DimitriosLekkas, "Addressing cloud computing security issues", Future Generation Computer Systems,Vol. 28, pp. 583-592, 2012.

[5] Cloud Security Alliance, March 2010, "Top Threats to Cloud Computing", Retrieved from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] JianhuaChe, YaminDuan, Tao Zhang, Jie Fan, "Study on the security models and strategies of cloud computing", Procedia Engineering, Vol. 23, pp. 586-593, 2011.

[7] Dawei Sun, Guiran Chang, Lina Sun, Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Procedia Engineering, Vol. 15, pp. 2852-2856, 2011.

[8] Yanpei Chen, Vern Paxson, Randy H. Katz,"What's New about Cloud Computing Security?", 2010,Retrieved fromhttp://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html

[9] Trend Micro, "Security Threats TO EvolvingData Centers", Retrieved from http:/www.trendmicro.com/cloud-content/us/pdfs/about/rpt_security-threats-to-datacenters.pdf

[10] DR. Werner Streitberger, Angelika Ruppel, "Cloud Computing Security", 2010, Retrieved from http://www.aisec.fraunhofer.de/content/dam/aisec/en/pdf/studien/studieCloudComputingSicherheit-AISEC-en.pdf

[11] Wikipedia, "Side channel attack"http://en.wikipedia.org/wiki/Side_channel_attack.

[12] Doug Hyde, "A Survey on the Security of Virtual Machines", 2009, Retrieved from http://www.cs.wustl.edu/~jain/cse571-09/ftp/vmsec/

[13] Kumar Dayanand, S.Magesh, "Defense Strategy against Flooding Attacks Using Nash Equilibrium Game Theory", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[14] UNIKEN Inc. "Security Manual", 2009, Retrieved from www.uniken.com/Whitepapers/Security_Manual.pdf