ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

A Survey of Intrusion Detection Systems in Cloud Computing

Kirti Ramhariya[1], Prof. Soumya Asati[2], Prof. Sumit Nema[3]

M.Tech. Student, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[2]

Assistant Professor and Head of The Department, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[3]

ABSTRACT: The distributed and open structure of cloud computing and services becomes an attractive target for potential cyber-attacks by intruders. The traditional Intrusion Detection and Prevention Systems (IDPS) are largely inefficient to be deployed in cloud computing environments due to their openness and specific essence. This paper surveys, explore about the most modern developed IDPSs and alarm management techniques by providing a complete classification and investigating possible solutions to detect and prevent intrusions in cloud computing systems. Considering the desired characteristics of IDPS and cloud computing systems, a list of useful requirements is identified and four concepts of autonomic computing self-management, risk management, and support vector machine are leveraged to satisfy these requirements.

KEYWORDS: Cloud Computing, Security, Vulnerabilities, Threats, Risks.

I. INTRODUCTION

Cloud computing is arguably one of the most significant technological shifts of our time. The mere idea of being able to use computing in a similar manner to using a utility, such as electricity, is revolutionizing the IT services world and holds great potential. Customers, whether large enterprises or small businesses, are drawn toward the cloud's promises of agility, reduced capital costs, and enhanced IT resources. IT companies are shifting from providing their own IT infrastructure to utilizing the computation services provided by the cloud for their information technology needs [1].

Cloud computing introduces a level of abstraction between the physical infrastructure and the owner of the information being stored and processed. Such indirect control of the physical environment introduces vulnerabilities unknown in previous settings. Such a radical change is of course not risk free. As IT services are contracted outside of the enterprise, the dependency on third party providers compels companies to rethink their risk management techniques and adapt accordingly.

After this brief introduction, the remainder of this paper is organized as follows: section 2 provides an overview of cloud computing, its services, and core technologies; section 3 provides a survey of known general risks, vulnerabilities and threats, and then explores the additional risks introduced by (or relevant to) cloud computing; section 4 provides some real world examples of vulnerabilities of cloud computing that have been reported in the literature; section 5 provides our conclusion and recommendations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

II. OVERVIEW OF CLOUD COMPUTING

As with any new technology, the definition of cloud computing is changing with the evolution of technology and its services. No standard definition for cloud computing has yet been agreed upon, especially since it encompasses so many different models and potential markets, depending on venders and services. In the simplest of terms, cloud computing is basically internet- based computing. The term "cloud" is used as a metaphor for the Internet, and came from the well known cloud drawing that was used in network diagrams to depict the Internet's underlying networking infrastructure. The computation in the internet is done by groups of shared servers that provide on demand hardware resources, data and software to devices connected to the net.

The National Institute of Standards and Technology NIST, gives a more formal definition: "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" [2]. NIST also notes that this definition will probably change over time.

In this sense, users of cloud computing are raised to a level of abstraction where they are hidden and relived from the details of the hardware or software infrastructures that supports their computations. This greatly simplifies the costs involved in establishing and managing the IT that is needed to meet the requirements of any business. And since businesses will pay only for the required IT resources when and as they are needed, more and much more powerful resources can be provided at a fraction of the price of the real value for such resources.

2.1 Core technologies

To better understand the security issues that are associated with CC, it is important to discuss the core concepts and technologies in cloud computing. CC is based on the general principle of utility computing – providing metered services of computing resources in a similar manner to the other utilities such as electricity. The measured service-oriented perspective for computing resources can be easily understood for the hardware resources. But this perspective can also be extended to software systems because they are designed and built in the form of autonomous interoperable services [3].

The large variety of devices that can connect to the internet, such as PDAs, mobile phones and handheld and static devices, all expanded the number of ways the cloud can be accessed. Coupled with acceptance of the browser as some sort of universal interface for even very complex systems, the potential of cloud computing could be tapped using basically any device that can load a browser. High speed broadband networks, data centers, and server farms are also critical components.

But perhaps the most influential concept in cloud computing would be virtualization. In computing, virtualization is the creation of a virtual (rather than actual) version of computers or operating systems. In this sense, the physical traits of the computing platform are hidden from the users and instead another abstract computing platform is presented. The software that creates this virtual environment is usually called a hypervisor. In case of server consolidation, many small servers with different OSs are substituted by one powerful server, and the previous operating systems are run in virtual environments on this server. The large server can "host" many such "guest" virtual machines which can be more easily configured and controlled. And this will allow the same hardware to present itself in different capabilities as the users need, a key concept in cloud computing.

2.2 Cloud Computing Main Characteristics Another way of defining cloud computing is to examine its characteristics, especially the ones that have been agreed upon and are generally accepted by different groups:

- Shared resources: or what NIST calls resource pooling, where no resources are dedicated to one user but instead are pooled together to serve multiple consumers. Resources whether on the application, host or network level, are assigned and reassigned as needed to these consumers. This creates a sense of location independence where users

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

cannot pinpoint exactly where there computations are being executed [2].

• On-demand self-service: the users can assign themselves additional resources such as storage or processing power automatically without human intervention. This is comparable with autonomic computing where the computer system is capable of self management.

• Elasticity: along with self provisioning of resources, cloud computing is characterized with the ability to locate and release resources rapidly. This will allow the consumers to scale up the resources they need at any time to address heavy loads and usage spikes, and then scale down by returning the resources to the pool when finished.

• Pay as you go: or what is known as measured service. Computing in the cloud is offered as a utility which users pay for on a consumption basis, not unlike any other utility enterprises pay for such as electricity, gas and water.

It could be argued that the main feature of cloud computing is that the computation is done in the "cloud" and remaining characteristics stem from or complement this simple fact. Additional characteristics have also been reported in the literature but most of these are, in our opinion, complementary to the main characteristics we reported above [4].

2.3 Cloud Computing Service models

The services provided by cloud computing can be categorized into three service models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These three models often abbreviated as the SPI Service framework (i.e. SPI is short for Software, Platform and Infrastructure) are the basis of all services provided by cloud computing:

• Software as a Service (SaaS): in this model software is provided by the vendor over the net as a one-to-many model (single instance, multi-tenant architecture) as a substitute of the one-to-one typical model. Instead of users buying the software and installing it on their systems, they rent the software using pay-per-use, or subscription fee. Thus the user exchanges the capital expense acquiring software licenses for operation expenses renting software usage. Since the application is provided over the net, usually the package includes the usage of the software itself and the utilization of the hardware it runs on, in addition to some level of support. Additional benefits of this model is centralized updating, so users don't need to worry about patching and versioning. Examples of SaaS would be Google Docs and Salesforce.com customer relationship Management CRM software.

• Platform as a Service (PaaS): the sophistication needed to create software that can run in the cloud entails the providers to create a development environment or platform on which these applications can be executed. The second service provided in the cloud is the utilization of the development environment itself. Users can create custom applications that target a certain platform, with tools offered by the platform provider. They then can deploy and run these applications on this platform, with full control over the applications and their configuration. Such applications may also be acquired from third parties. When using this service, users don't need, or even have the ability to manage the underlying cloud infrastructure, including servers, storage mediums and network configuration. The benefits of such a service are large, since startup companies and small teams can start developing and deploying their own software without the need to acquire servers and teams to manage them. Examples of PaaS would be Google's Apps Engine and Microsoft's Azure Platform.

• Infrastructure as a Service (IaaS): in the third service, the users are given access to elements of the computing infrastructure itself. Using internet technologies, users can utilize the processing power, storage mediums and necessary networking components provided by the vendor. Users then can run arbitrary software and operating systems that best meets their requirements, with full control and management. This is much like traditional hosting services except when done in the cloud it is possible to scale the service to conform to the changing requirements, and to offer the pay per use model. This model is very similar to utility computing where users pay for the consumption of disk space, processing power, or bandwidth they use. Examples would be Amazon.com, EC2 and S3.

III. CLOUD COMPUTING RISKS, THREATS & VULNERABILITIES

The words "Vulnerability," "Threat," "Risk," and "Exposure" often are used to represent the same thing even though they have different meanings and relationships to each other. It is important to understand each

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

word's definition, but more important to understand its relationship to the other concepts.

"Vulnerability" refers to a software, hardware, or procedural weakness that may provide an attacker the open door to enter a computer or network and have unauthorized access to resources within the environment. Vulnerability characterizes the absence or weakness of a safeguard that could be exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software, or an unsecured physical entrance.

A "Threat" is any potential danger to information or systems. The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual. Threats exploit existing vulnerabilities in an attempt to cause damage or destruct a resource. A "Threat Agent" is the entity that takes advantage of vulnerability. A threat agent could be an intruder, a process, or an employee making an unintentional mistake that could expose confidential information or destroy a file's integrity.

A "Risk" is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact. For example, if users are not educated on processes and procedures, there is a higher likelihood that an employee will make an intentional or unintentional mistake that may destroy data. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact (see Figure 1).

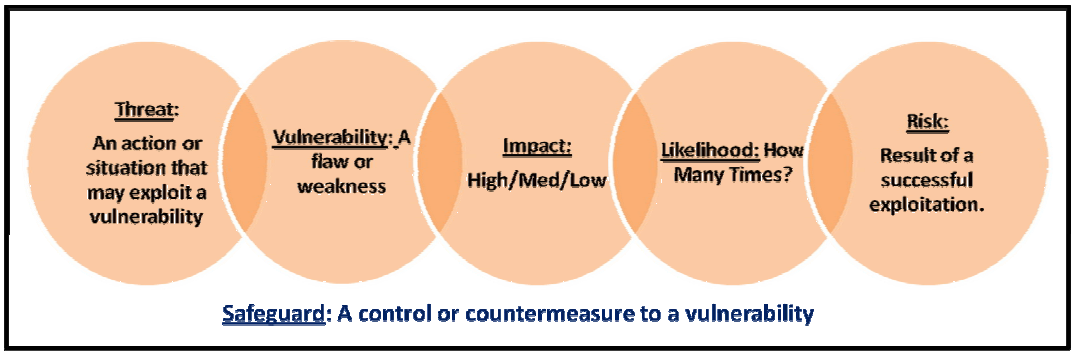

Figure 1. Risk = Vulnerability x Threat x Impact x Likelihood.

An "Exposure" is an instance of being exposed to losses from a threat agent. Vulnerability exposes an organization to possible damages. If a bank does not properly patch its servers then it may be exposed to possible breaches in relation to the open holes resulting from the missing patches.

A countermeasure (also referred to as a safeguard) is generally put into place to mitigate the potential risk. A countermeasure may be a policy, procedure, a software configuration, or a hardware device that eliminates vulnerability or reduces the likelihood that a threat agent will be able to exploit a vulnerability. Strong authentication mechanisms, computer anti- virus software and information security awareness are some examples of proper countermeasures.

In any enterprise, information security risks must be identified, evaluated, analyzed, treated and properly reported. Businesses that fail in identifying the risks associated with the technology they use, the people they employ, or the environment where they operate usually subject their business to unforeseen consequences that might result in severe damage to the business.
Because risks cannot be completely eliminated, they need to be lowered into acceptable levels. Acceptable risks are risks that the business decides to live with, given that proper assessment for these risks was done and the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

cost of treating these risks might outweigh the benefits.

As we discussed above, CC is in reality a business model in which companies with limited resources to build their own IT infrastructure elect to outsource this to third parties who will in turn lease their infrastructure and probably applications as services. Thus, the risks, threats and vulnerabilities that are usually associated with technology in general exist in this environment, because outsourcing the technological service only transfers the liability. In addition, this new model introduces more security challenges due to mainly the fact that the data is on the cloud (i.e. hosted somewhere in the Internet space), being transferred across countries with different regulations, and most importantly might reside on a machine that hosts other data instances of other enterprises. In some instances, the data for the same enterprise might even be stored across multiple data centres. We will concentrate on the cloud-specific security issues (see Figure 2 below).

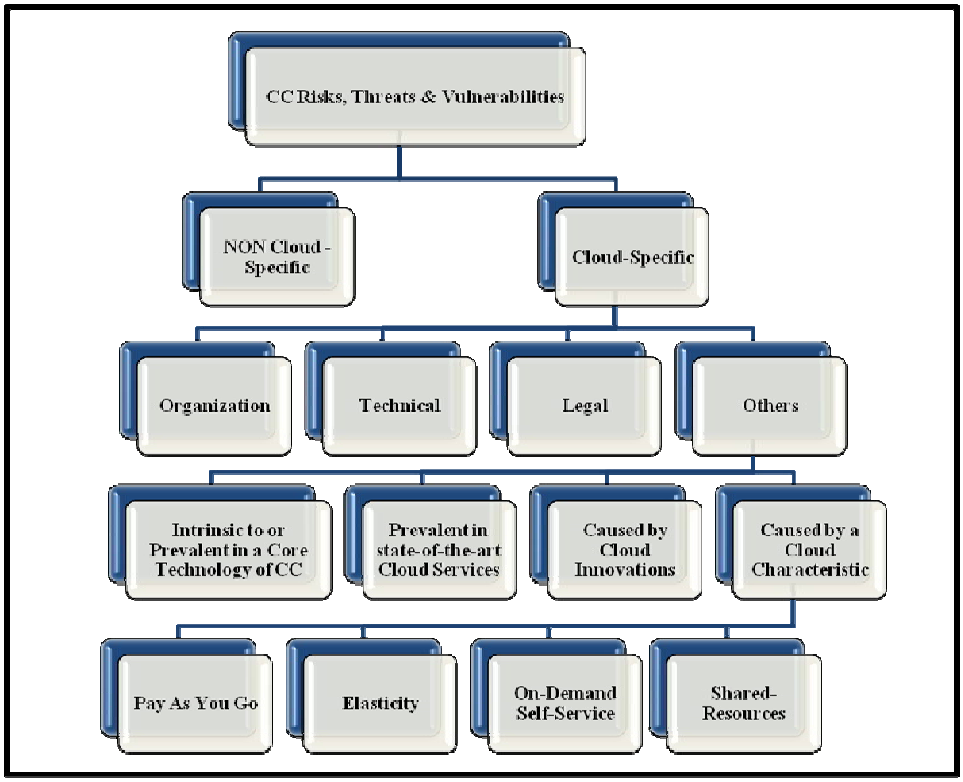

Figure 2. Cloud Computing Risks, Threats & Vulnerabilities.

3.1 Risks and Threats in the Cloud

Information security risks in Cloud Computing (CC) were subject for detailed analysis and assessment. One of the best efforts in this direction was realized by the European Network & Information Systems Agency (ENISA) whom developed a comprehensive detailed research in this regards [5]. Other groups such as Cloud Security Alliance (CSA) who specialize in cloud computing technology and information security matters also have significant publications [6]. ENISA classifies Cloud Computing (CC) risks into three categories: Organizational, Technical and Legal. CSA threats model avoids classifying CC's risks but yet introduce a detailed list of considerable issues that need to be properly addressed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

The organizational risks classification includes all risks that may impact the structure of the organization or the business as an entity. Examples of such risks include, but not limited to, loss of business reputation due to co-tenant activities (or the tenants sharing the same resource), and any organizational change that can happen to the cloud provider (as a business organization) including provider failure, termination or acquisition.

The technical risks classification includes problems or failures associated with the provided services or technologies contacted from the cloud service provider. Examples of such risks include, but not limited to, resource-sharing isolation problems, malicious (insiders or outsiders) attacks on the cloud provider, and any possibility of data leakage on download/upload through communication channels.

The legal risks classification refers to issues that surround data being exchanged across multiple countries that have different laws and regulations concerning data traversal, protection requirements and privacy laws. Examples of such risks include, but not limited to, risks resulting from possible changes of jurisdiction and the liability or obligation of the vendor in case of loss of data and/or business interruption.

Cloud Computing is based on a new utilization of technology and many risks that used to be present in other technological implementations do still exist, and are realized as not cloud specific. Risks like social engineering, physical security, lost or stolen backups, and loss or compromise of security logs are just a few examples of such general security risks.
The Cloud Security Alliance (CSA) lists the following threats as the top risks associated with CC based on their recent research: malicious insiders, data loss/leakage, abuse and nefarious use of CC and shared technology vulnerabilities [6]. Even though CSA prefers to prioritize risks, it easy to see that each of the listed threats can be included in the ENISA categories or as non-cloud specific, or general, security risk.

3.2 Cloud Specific Vulnerabilities

Other researchers prefer to focus on cloud specific vulnerabilities, without much focus on threats and risks [7].
According to such research, a particular vulnerability can be considered specific to cloud computing if it meets any of the following criteria:

- it is intrinsic to or prevalent in a core technology of cloud computing, such as virtualization, service-oriented architecture, and cryptography
- it has its root cause in one of essential cloud characteristics, such as elasticity, resource pooling, and pay-as-you-go model
- it is caused by cloud innovations making exiting (tried and tested) security controls hard or impossible to implement; for example, management procedures that were created initially for a fixed hardware structure do not port correctly to virtual machines [5]
- it is prevalent in established state-of-the-art cloud services

IV. REAL WORLD EXAMPLES

Many of the cloud specific vulnerabilities, the threats that might exploit them, and the risks associated with them have appeared as actual incidents. The following section will present some real world examples of cloud specific vulnerabilities and whether they have been exploited or not. This is by no means a comprehensive list, but is primarily intended to highlight the main security issues that might accompany cloud computing technologies.

4.1 Using IaaS to Host Crimeware

In its low level offering, cloud computing rents out storage space, processing cycles, and network components to consumers, allowing them to utilize them in whatever manner they wish within certain constraints. In the case of the certain cybercriminals, the cloud's IaaS was used as a platform to control a malicious botnet derived from the crimeware Zeus.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

The Zeus crimeware toolkit is well established in the underground economy as being an easy to use and powerful tool for stealing personal data from remote systems. Based on the do- it-yourself DIY model, the crimeware allows entry level hackers to create their own versions of botnets. As in any botnet, there is a need to be able to communicate and command all the computers infected with it. In 2009, security experts uncovered a variant of Zeus using Amazon's EC2 IaaS to command and control their botnets [8]. Even though using an ISP might offer better anonymity, using a cloud can provide traffic camouflaging, where it would be harder to detect and blacklist harmful activity that is hiding in traffic disguised as a valid cloud service.

4.2 The Blue Pill Rootkit

As mentioned before, cloud computing is primarily based on the concept of virtualization, Therefore, strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider [5]. But virtual machine escape would not be the only problem stemming from virtual environments. In 2006 Joanna Rutkowska, a security researcher for IT security firm COSEINC, claims to have developed a program that can trick a software to think that it is running on a certain system, where in reality it is running on a virtual version of this system [9]. This rootkit which is coined the "blue pill" creates a fake reality for an entire operating system and all of the applications running on it including anti- malware sensors. The risk of such a program is that it could easily intercept all hardware requests from any software running on the system. The creators of the blue pill claim it to be completely undetectable, although some have disputed this claim [10]. Whether detectable or not, it would hard not to acknowledge that it demonstrates how exploits can be developed based on virtualization technologies.

4.3 Cloud Computing Outage and Data Loss Leading providers of cloud computing services have suffered, and in some cases more than once, from data loss or suspension of service. The following are just a few examples of such incidents:

- In 2009 Salesforce.com suffered an outage that locked more than 900,000 subscribers out of crucial CC applications and data needed to transact business with customers. Such an outage has even greater impact on companies with most of their operations conducted within the cloud [11].
- In September 2009 an estimated 800,000 users of a smart phone known as "Sidekick" temporary lost personal data that they could access from their smart phones. The outage lasted almost two weeks and some losses might have been were permanent. The data at the time was stored on servers owned by Microsoft, and accessed as a cloud service. At the time it was described as the biggest disaster in cloud computing history [12].
- Rackspace was forced to pay out between $2.5 million and $3.5 million in service credits to customers in the wake of a power outage that hit its Dallas data center in late June 2009.

V. CONCLUSION

Cloud Computing is an exciting new IT frontier which holds great potential and introduces many benefits for many organizations. The need to understand what CC is, its capabilities and associated vulnerabilities and risks are imperative if enterprises are to make the shift towards outsourcing, and trusting, their computations to the cloud. Many security measures should be taken such as conducting security assessments and having deep understanding of related laws, regulations and best practices to ensure that the right cloud provider is selected. The selection of cloud service provider is very crucial; cloud computing providers should be selected carefully with focus on solid reputation and clear and comprehensive contracts. Companies should also develop solid Business Continuity (BCP) plans and have them tested, and have continuous monitoring software solutions.

Cloud computing is great to use but needs to be considered very carefully. Several risks need to be accounted for and addressed through proper controls to deal with its legal, technical and organizational risks. Deciding to do business on the cloud is a shared responsibility between business and IT. Therefore, proper alignment between business objectives and IT needs to be carefully well thought-out. Transferring risk through outsourcing to a cloud-service provider should not eliminate responsibility, and due diligence and due care must always be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

practiced.

REFERENCES

[1] Nicolas Carr, The Big Swtich Our New Destiney ; W. W.Norton & Co., 2008.
[2] NIST, "NIST.gov - Computer Security Division - Computer Security Resource Center". DOI=http://csrc.nist.gov/groups/SNS/cloud-computing/.
[3] Yi Wei and M. Brian Blake, "Service-Oriented Computing and Cloud Computing: Challenges and Opportunities", IEEE Internet Computing, vol. 14, no. 6, pp. 72-75, Nov.-Dec. 2010,
[4] Tim Mather, Subra Kumaraswamy, and Shahed Latif, “Cloud Security and Privacy”, s.l. ; O'Reilly, 2009.
[5] ENISA, Cloud Computing: Benefits, risks and recommendations for information security, 2010.
[6] CSA. Top Threats to cloud computing v1.0, 2010.
[7] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities", IEEE Security and Privacy, 10 Jun. 2010, IEEE computer Society Digital Library, IEEE Computer Society
[8] Zeus crimeware using Amazon's EC2 as command and control server, DOI= http://www.zdnet.com/blog/security/zeus-crimeare- using-amazons-ec2-as-command-and-control- server/5110.
[9] The Blue Pill, DOI= http://theinvisiblethings.blogspot.com/2008/07/0wning- xen-invegas.html.
[10] Rutkowska Faces, “100% undetectable malware' challenge”, DOI= http://www.zdnet.com/blog/security/rutkowska-faces-100-undetectable-malware-challenge/334.
[11] Salesforce.com outage hits thousands of businesses, DOI= http://news.cnet.com/8301-1001_3-10136540-92.html.
[12] BBC, The Sidekick Cloud Disaster, DOI= http://www.bbc.co.uk/blogs/technology/2009/10/the_side kick_cloud_disaster.html.
[13] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning, Managing Security of Virtual Machine Images in a Cloud Environment, ACM Cloud Computing Security Workshop (CCSW’09).
[14] Kleber Vieira, Alexandre Schulter, Carlos Westphall, Carla Westphall, Intrusion Detection Techniques in Grid and Cloud Computing Environment, IT Professional, IEEE Computer Society, 8/2009.
[15] Niels Provos, Moheeb Abu Rajab, Panayiotis Mavrommatis, Cybercrime 2.0: When the Cloud Turns Dark, Communications of the ACM, 4/2009.
[16] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, On Technical Security Issues in Cloud Computing, IEEE International Conference on Cloud Computing, Bangalore, India 9/2009.
[17] Siani Pearson, Taking Account of Privacy When Designing Cloud Computing Services, International Conference on Software Engineering (ICSE) Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, 5/2009.
[18] Michael Armbrust et al., A View of Cloud Computing, Communications of the ACM, Association for Computing Machinery, Vol. 53, No. 4, 4/2010.
[19] David S. Ferreiro, Guidance on Managing Records in Cloud Computing Environments, NARA Bulletin 2010-05, DOI= http://www.archives.gov:80/records- mgmt/bulletins/2010/2010-05.html.
[20] Joanna Rutkowska, Security Challenges in Virtualized Environments, white paper, Nordic Virtualization Forum, 10/2007.
[21] Lamia Youseff, Maria Butrico, und Dilma Da Silva, Towards a Unified Ontology of Cloud Computing, in Proceedings of Grid Computing Environments Workshop (GCE) 2008. DOI= http://www.cs.ucsb.edu/%7Elyouseff/CCOntology/Cloud Ontology.pdf.
[22] European Network and Information Security Agency (ENISA), Cloud Computing: Benefits, risks and recommendations for information security, 11/2009
[23] Hobson, D. Global Secure Systems: Into the Cloud we go.....have we thought about security issues? DOI= http://www.globalsecuritymag.com/David-Hobson- Global-Secure-Systems, 20090122, 7110. 1/2009.