International Journal of Advanced Computer Technology (IJACT)
ISSN: 2319-7900 www.ijact.org Volume IX, Issue IV, July-August 2020

Managing Cyber Risk and Security In Cloud Computing

Jahid Sheikh, Bhupendra Malviya
CSE Department, SORT Peoples University, Bhopal
[1]jahidsheikh@gmail.com, [2]bhupendra09sm@gmail.com

Abstract—*Cloud computing provides outsourcing of resources bringing economic benefits. The outsourcing however does not allow data owners to outsource the responsibility of confidentiality, integrity and access control, as it still is the responsibility of the data owner. As cloud computing is transparent to both the programmers and the users, it induces challenges that were not present in previous forms of distributed computing. Furthermore, cloud computing enables its users to abstract away from low-level configuration such as configuring IP addresses and routers. It creates an illusion that this entire configuration is automated. This illusion is also true for security services, for instance automating security policies and access control in cloud, so that individuals or end-users using the cloud only perform very high-level (business oriented) configuration. This paper investigates the security challenges posed by the transparency of distribution, abstraction of configuration and automation of services by performing a detailed threat analysis of cloud computing across its different deployment scenarios (private, bursting, federation or multi-clouds). This paper also presents a risk inventory which documents the security threats identified in terms of availability, integrity and confidentiality for cloud infrastructures in detail for future security risks. We also propose a methodology for performing security risk assessment for cloud computing architectures presenting some of the initial results.*

Keywords-security threats; risk assessment; cloud computing

I. INTRODUCTION

Cloud computing has been promoted as a new paradigm and the 5th utility service after water, electricity, gas and telephony [7, 11]. In the past, enterprises supported their business by procuring IT infrastructure and developing their software on top of that infrastructure. Cloud computing presents a model in which IT infrastructure is leased and used according to the need of the enterprise. The benefit of this model is that it converts capital expenditure of an enterprise into operational expenditure [5]. The most comprehensive definition of cloud computing was made by National Institute of Standard and Technology (NIST) [12] where cloud is described as a convenient model using efficient computing resources stressing on four deployment models. *Private cloud* is solely operated for an organization by either itself or a third party. Public cloud is available for general public use and is owned by an organization selling cloud services. Community cloud provides an infrastructure that is shared by several organizations, also called federation of clouds. Hybrid cloud is a composition of two, more clouds or multi-clouds (community, private, public).While cloud computing is another way of implementing distributed systems; it is unique such that the infrastructure is transparent to users and programmers alike. This allows new ways of selling and sharing resources altogether. Cloud computing offers a new economic model which enables enterprises to shift from the conventional way of developing their own IT departments to outsourcing their needs of software, platform and infrastructure. We envision that this shift would enable hybrid clouds to become a commonplace, realized by private clouds interacting with a rich eco system of various different types of cloud. We are already witnessing research being conducted to enable organizations to automatically externalize services and applications to trustworthy and auditable cloud providers in the hybrid model [6].

Each of these deployment scenarios can bring a number of challenges in various aspects of the clouds like risks on the infrastructures, data protection or security. Across these models, security requirements can be associated with interoperability, reliability, portability, maintainability, availability, integrity and confidentiality. These will also differ depending on the point of view of the involved actors; for instance, the end user or cloud consumer may have concerns about their data usage, whereas the service providers would be concerned over malicious intent. Various policies for authentication and software assurances are used to build confidence of customers to use clouds. This paper presents the security issues faced in cloud computing and analyses it as a risk measure of the providers involved in the cloud – the service provider (SP) and the infrastructure provider (IP). Section II explains the motivation and presents the background for the security issues that need to be addressed in clouds. Section III explains a systematic approach for threat analysis based on standard threats for distributed systems, adopted in cloud computing. The methodology discussed uses the CORAS risk modelling methodology [3] coupled with Information Risk Analysis Methodology (IRAM), using the Threat and Vulnerability Assessment tool (T&VA) performed using data provided by the Information Security Forum (ISF) [9] and public data [12] tailoring for specific cloud computing security risk assessment. This research is exploited into a risk model for security and presented in Section IV with an evaluation of the suggested methodology. The results have been based on the implementation work carried out in an EU-project OPTIMIS [6] presenting analyses across different deployment scenarios. Section V presents related security research in cloud computing. Finally Section VI presents the conclusions of the risk modelling methodology and future research directions to adopt using it.

II.PROBLEM STATEMENT

Computer and information security are concerned with ensuring the availability, integrity and confidentiality of information. Availability is concerned with the information being accessible when needed, whereas integrity refers to not allowing data to be modified without being undetected. Confidentiality is concerned with the disclosure of data to unauthorized personnel.

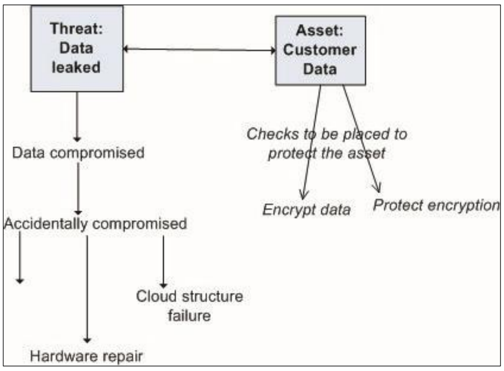


Figure 1: Example of a security threat analysis for data loss

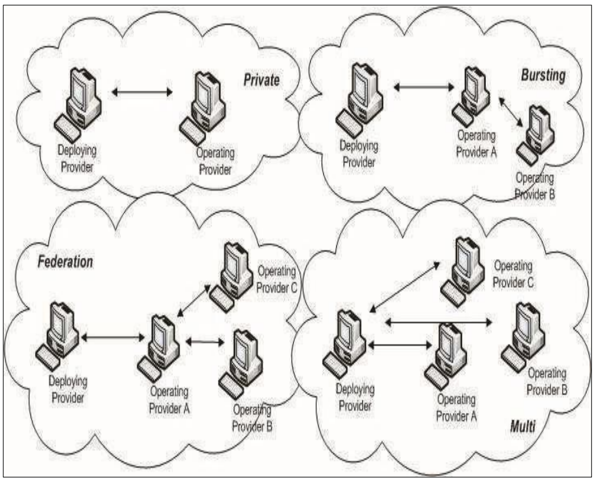


Figure 2. Cloud scenarios. (Private involves one deploying and one operating provider, bursting - the operation provider can burst to another provider, federation - a team of providers work together, multi - the service can be deployed on a number of providers, acts as a broker)

Each of these aspects covers an integral part of security aspects of the infrastructure. In cloud computing, security is one of the highest concerns as it can make or break deals by either convincing organizations to use or deferring its use on security concerns. For instance, Microsoft [4] employs a threat modelling technique to keep security concerns intact, while [1] discusses how security needs an in-depth threat analysis to be done for every unit in the system. Others [2] have identified policies and control, knowledge and performance management by using risk, audits, SLA monitoring and protection policies for clouds. Threat analysis helps create a preliminary investigation protecting various assets and prevent certain threats from happening. Figure 1 depicts an example of the analysis of a data loss threat identifying assets and protection techniques such as security audits and hardware wipe policies. The different cloud deployment scenarios raise different kinds of threats depending on how the service executes on the infrastructures. These have been depicted in Figure 2.

III.PROPOSED SOLUTION

Risk analysis can be considered at various phases of interactions in clouds (Figure 3). Each provider involved in the cloud will have security concerns from their own point of view towards the others in terms of trust [22], service risks or legal issues. They might consider the risk of working with other providers or may have specific security demands that need to be honoured. These assessments also depend on the cloud deployment scenarios - private, public or hybrid.

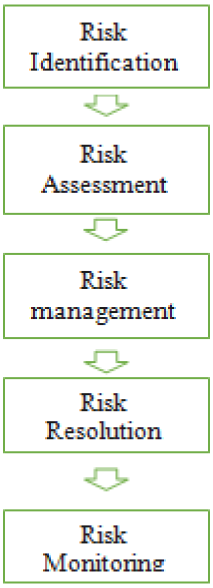


Figure 3. Risk assessment lifecycle during service deployment/operation

These concerns can also be refined depending on the stage of the cloud lifecycle – deployment or operation. Risk needs to be assessed at service deployment stage for initial placement of services on cloud providers, and the service operation, where cloud resources and data are managed by the cloud provider to fulfil the Service Level Objectives. During deployment and operation stages, risk needs to be constantly monitored in order to prevent any additional costs to be incurred to the end-users and cloud providers. A number of stages have been identified for performing a complete risk assessment on clouds by considering core risk assessment approaches as explained below:

A. High level analysis of the system

An initial high-level analysis of the deployment scenarios helps identifying the actions and assets involved at the different stages in the cloud. This helps isolate the assets involved and how they change over time to identify the vulnerabilities of the cloud environment. Generally security needs to be assessed before deployment of the service to check for security concerns of the other provider or if service level agreements (SLAs) demand certain security aspects to be met (Figure 3). During the operation, security concerns are monitored while the service is executing.

B. Identifying the assets involved

There are various assets involved either at the deployment or operation stage such as the SLA or customer data. These can be monitored in relation to the specific threats in the environment.

C. Identify the threats in each cloud deployment scenario

Threat modelling is a systemic approach by which threats and vulnerabilities of a system can be identified. The information risk analysis methodology is coupled with the threat and vulnerability assessment tool (T&VA) because it contains a threat model for distributed systems and software in general. This model has been adapted to cloud applications using the CORAS risk modelling technique [3]. We have adapted a formal risk methodology, CORAS to further substantiate and filter the threats coming in from the T&VA.

In this paper, threat classification is based on two sources of information, the information security forum [38] for providing data on attacks on IT systems and the frequency of attacks and the public data on attacks on the cloud platforms such as Amazon EC2 and Google Apps Engine. The T&VA [36] Provides a standard list of threats relating to IT systems, adopting the threats relevant to the cloud deployment scenarios being investigated. Further threats have been added to introduce the differences between cloud computing and other forms of distributed computing. These have been listed in Table 1. The main threats are *Data Leakage, Usage Control* and *Hypervisor level attacks* and these have been classified into the following six categories:

1. *External attacks:* These include all the threats in scenarios involving use of public infrastructures. Examples include problems with Amazon public cloud [40], using audits such as that of SAS type 2 audit [20] and ISO 27001 [24]. These threats can lead to loss of confidentiality and integrity as multiple enterprises using provider services require development of technical and legal safe guard for the protection of identities. In [39] attack services are defined in which cloud platforms can be infected with malicious code. An example is Bluepill that can infect hypervisor which can then be used to control the virtual machines (VMs) [41]. In Amazon EC2 cloud, it was used to distribute spam which lead to the banning of EC2 related IP addresses by anti spam groups [27].

2. *Theft:* Cloud computing supports multi tenant architecture in which multiple users can consume the same computing resources allowing possible theft of data. Potential adversaries can use advance data recovery tools to recover data owned by other customers. Google in its security data sheet mentions that only references to the data are deleted rather than data itself. The likelihood of this threat being exploited is low but some companies employ high end physical security measures to secure data.

3. *System malfunction:* A bug in the cloud software used can have adverse consequences. The likelihood of this threat is high and is classified as one of the most frequent.

4. *Service interruption:* Natural disasters like earthquakes can lead to the interruption of service

5. . *System overload* causes excessive system activity leading to the degradation of performance such as the unavailability of services. Although theoretically, cloud computing offers unlimited amount of computing resources, it still depends on how the websites or the cloud services are configured and the availability zone they reside in. Wikileaks used EC2 platform to host their website, protecting against DoS attacks by paying a high end package to protect their website. The threat is difficult to recognize as it is challenging to distinguish between a genuine peaks in demand for usage of cloud services with a DoS attack as both create similar patterns of data usage. ***5. Human error:*** Infrastructure providers like EC2 have designed automated systems with no human intervention for provisioning of cloud services. However, once provisioned human errors cannot be controlled. It is hard to predict human behaviour. Therefore we classify this threat as a high threat [9]. Google Apps in its SLAs promise 0.01% for data outages but does not take responsibility for data loss due to human error The IT policy compliance group suggests that 75% of all data loss is due to user error

6. System specific threats and abuse: Data Leakage is defined as an unauthorized transmission of data (or information) from within an organization to an external destination or recipient, in electronic form or by a physical method

. This threat becomes more critical in cloud environments as enterprises who are hosting their data on clouds have no control over the provider's infrastructure. In cloud specific environments where data from multiple enterprises may reside in the same data centre, it is necessary to build controls for data access. This threat has been classified as *medium* by GoogleDocs. *Hypervisor level attacks* enable an adversary to exploit vulnerability at the virtualization layer that is running underneath the VMs. There are numerous attacks that have been recorded at the hypervisor level ranging from the injection of malware to the hijacking of a VM by a thin undetectable hypervisor, classifying this as a high threat

Table 1 lists the various threats identified along with the stage of the cloud lifecycle these threats may be active. The table also includes the classification of the threats in confidentiality, availability and integrity using the information risk rating.

D. *High-level analysis of each threat*

Each of the threats can be further analyzed in terms of who causes them and the incidents leading up to them, which can then be prioritized depending on this information. This also helps measure the impact of the security risk on the service and the providers. Figure 4 depicts an example of the hacking threat and its related asset and vulnerabilities.

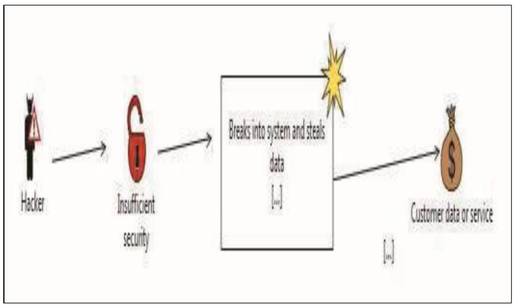
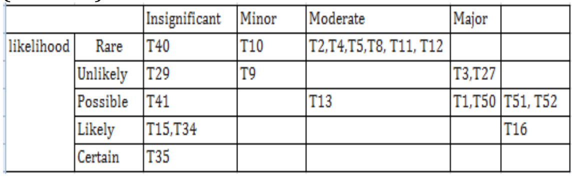


Figure 4. Analysing the threat *Hacking*

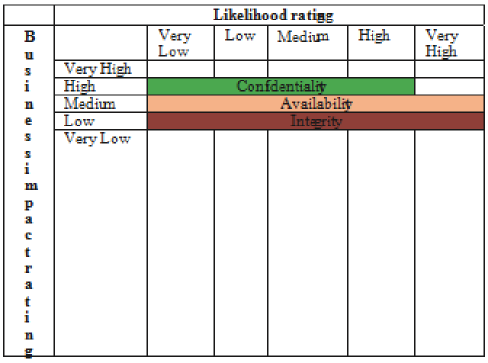
E. *Risk Evaluation*

Depending on the priority of the assets and likelihoods of the threats occurring, the threat items can be plotted into an evaluation matrix to document their occurrences. Table 2 depicts this in relation to the threats identified in Table 1. The likelihood and impact rating is set using the data collected [9, 12]. The impact also denotes the affect the threat will have on the business such as loss of confidentiality can cause loss in trust having the highest impact (Table 3).



		Insignificant	Minor	Moderate	Major	
likelihood	Rare	T40	T10	T2,T4,T5,T8, T11, T12		
	Unlikely	T29	T9		T3,T27	
	Possible	T41		T13	T1,T50	T51, T52
	Likely	T15,T34				T16
	Certain	T35				

Table 2: Risk evaluation matrix



<table>
<tr><td></td><td colspan="6">Likelihood rating</td></tr>
<tr><td rowspan="6">Business impact rating</td><td></td><td>Very Low</td><td>Low</td><td>Medium</td><td>High</td><td>Very High</td></tr>
<tr><td>Very High</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>High</td><td colspan="4">Confidentiality</td><td></td></tr>
<tr><td>Medium</td><td colspan="5">Availability</td></tr>
<tr><td>Low</td><td colspan="5">Integrity</td></tr>
<tr><td>Very Low</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Table 3: Range of threats for Confidentiality, Availability and Integrity

Threats belonging to confidentiality are classed as high because these have severe effect on trust and the provider's image. Loss of confidentiality can also convert low threats like theft of information to very high. For instance losing unencrypted data is a more severe risk compared to loss of encrypted data.

Loss of availability is relatively classified as medium compared to loss of confidentiality. This is because enterprises are better off using infrastructure provider's resources rather than deploying their own because of the investment involved. Examples include Bitbuket website continuing the use the EC2 even when further attacks are recorded.

Integrity is classed as low because relative to confidentiality and availability the impact is much lower. Loss of integrity can be because of software error, user error, and equipment failure and also due to an adversary changing data. From the recorded attacks on cloud platforms, it is difficult to find the reasons for the threats; additionally the VMs can also be restarted and redeployed on different infrastructures to counteract these threats.

F. *Risk Treatment*

Once evaluated, the risk mitigation strategies can be generated in terms of the actions taken to resolve them. These can be to accept, treat or outsource the risk. For instance, in a situation of multiple login, the system logs can be scanned to detect this. Once observed the system administrator can be made aware to take appropriate action on the user account.

IV.SIMULATION &IMPLEMENTATION

Security risk assessment needs to be done at the service deployment and operation stages of the infrastructure provider's (IP) cloud lifecycle. Figure 5, 6 describes the architectural details of the risk components involved at deployment and operation stages of the cloud lifecycle.

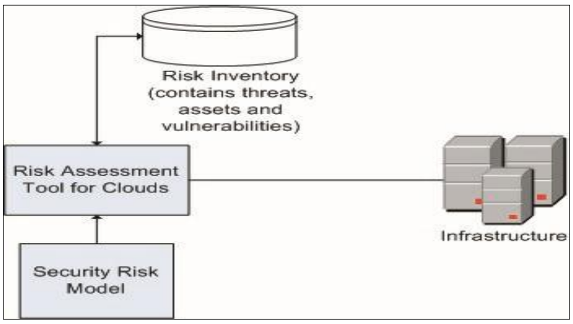

Risk Inventory (contains threats, assets and vulnerabilities)
Risk Assessment Tool for Clouds
Infrastructure
Security Risk Model

Figure 5. Security risk assessment at the deployment stage of the cloud

At the deployment stage, the risk assessment tool will read inputs from the risk inventory which documents all the threats, the vulnerabilities, assets affected and their likelihoods. The risk inventory is based on the threats collected in Table 1. Based on this information, security risk can be calculated as:

```
Security_risk_deployment (usecase)
1. Calculate the number of threats recorded at
   deployment stage and usecase
2. For each threat:
a. probability of likelihood given asset affected (p(B|A))
   = likelihood/ 5.0
b. probability of asset priority (p(A)) = priority/5.0
c. probability of likelihood regardless of asset (p(B))=
   p(B|A) * p(A) + p(A') *1
d. probability of threat occurring (p(A|B)) = ((p(B|A) *
   p(A))) / p(B)
3. Security risk = Sum all probabilities of threats
   occurring / threats found
```

Based on rules of Bayesian dependencies, the probability of each threat affecting the particular assets can be calculated before making the decision to accept the service by the IP.

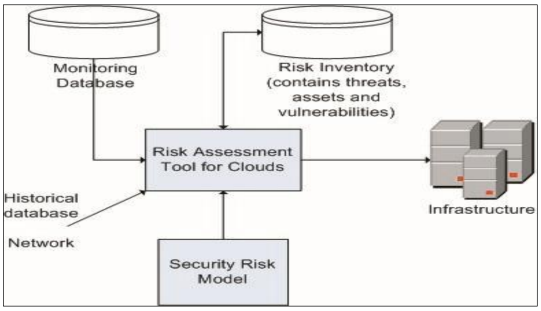

Monitoring Database
Risk Inventory (contains threats, assets and vulnerabilities)
Risk Assessment Tool for Clouds
Historical database
Network
Infrastructure
Security Risk Model

Figure 6. Security risk assessment at the operation stage of the cloud

However at the operation stage, along with the calculated security risk for this stage, the risk assessment tool will be interacting with the monitoring database and additional tools like the network and historical database to monitor if certain threats are becoming live. The stages 1-2 are similar to the deployment stage but in addition new stages are added for operation phase. The historical database can contain details of previously recorded threats that have occurred in the past. The network can include intrusion detection systems and logs which can be parsed to find out if certain events have been recorded [22].

```
Security_risk_operation (usecase)
3. Security risk = Sum all probabilities of threats
   occurring / threats found
4. For each threat to be monitored:
    4a. Read monitoring inputs
    4b. If (event found==true) count ++
5. Calculate total_event_rate= events_found/ total
   monitored time
6. Relative risk (RR)= total_event_rate/ security risk
7. If RR=1 do nothing, RR<1 accept risk, If RR>1 apply
   mitigation strategy
```

Depending on the value of relative risk (RR), the components can make a decision whether to accept or apply a mitigation strategy stored in the risk inventory to compensate for the risk. The risk is mitigated during the same time period. Figure 7 shows the output of 20 simulated samples collected while executing the risk model during the operation phase. Depending on the event rate per sample the relative risk can be calculated according to the algorithm step 6. If the relative risk is less than 1, the software can choose to accept the risk but if higher, the mitigation strategy will get activated which may ask for human intervention as the risk is going high.

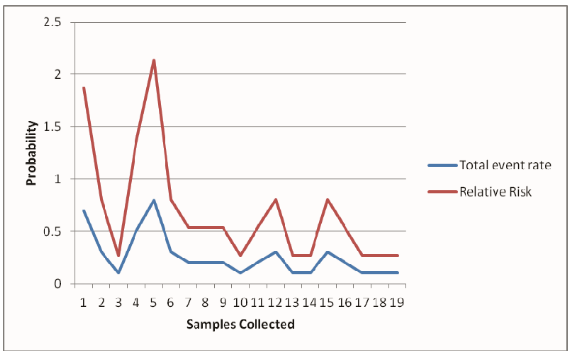


Figure 7: Calculating relative risk using samples and event rates. An action is taken when relative risk is more than 1.

V. CONCLUSION

From the threat analysis performed, we have shown that the information security principles of integrity, confidentiality and availability are most relevant to the cloud related scenarios. The information risk ratings performed shows the loss of confidentiality is rated as the highest level of risk followed by availability and integrity. For each of the threat categories the common research issues identified are:

- Scalable fine granular access control and data confidentiality in cloud computing scenarios.
- Using an intrusion detection system (Identification of user behaviour) to prevent data leakage at the infrastructure provider level.
- Detection of malware on virtual machines, from the hypervisor level by performing static and dynamic analysis.
- Identification of vulnerabilities at the hypervisor when giving API level access to the introspective layer of the hypervisor to the programmers.
- Security architecture for a hypervisor using the Usage control model [8].

The risk model presented here allows monitoring threats based on the events being logged by the detectors leading to a calculation of the relative risk. However, a fine granular analysis needs to be performed on threats which are difficult to detect via certain events or have a cause and effect relationship to other threats. These may be more specific to confidentiality or integrity classifications of the threats.

Further future work includes testing this system on a cloud platform with monitoring agents installed which will log certain threats when they occur. This will then be extended to work on determine threats which may be eventually seen based on the data being collected and difficult to determine directly from the events. Finally the results from the initial testing and evaluation, advocate that the risk model does correctly assess and prioritize the risk.

REFERENCES

[1] Draft NIST Special Publication Guidelines on Security and Privacy in Public Cloud Computing, Wayne Jansen, Timothy Grance, Computer Security, January 2011

[2] Derek Brink, Security and cloud best practices July 2011, Aberdeen

[3] The Coras Model-based method for security risk analysis, Folker den Braber, GyrdBrændeland, Heidi E. I. Dahl, Iselin Engan, Ida Hogganvik, Mass S. Lund, BjørnarSolhaug, KetilStølen, Fredrik Vraalsen, SINTEF, Oslo September 2006

[4] R. Buyya, C. S. Yeo, S. Venugopal, Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as

Computing Utilities, Keynote Paper, Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, pp. 5-13, 2008

[5] Cloud Computing: Special theme, European research consortium for Informatics and mathematics (ERCIM), ISSN 0926-4981

[6] A. Juan Ferrer, F. Hernandez, J. Tordsson, E. Elmroth, C. Zsigri, R. Sirvent, J. Guitart, R.M. Badia, K. Djemame, W. Ziegler, T. Dimitrakos, S.K. Nair, G. Kousiouris, K. Konstanteli, T. Varvarigou, B. Hudzia, A. Kipp, S. Wesner, M. Corrales, N. Forgo, T. Sharif, and C. Sheridan, OPTIMIS: a Holistic Approach to Cloud Service Provisioning, Proceedings of 1st International Conference on Utility and Cloud Computing (UCC 2010), Chennai, India, December 2010.

[7] R. Buyya, C.S Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th utility. Future Generation Computer Systems, 25, 599 – 616, 2008

[8] R. Sandhu, J. Park, Usage Control: A Vision for Next Generation Access Control Lecture Notes in Computer Science, 2003, Volume 2776/2003, 17-31, DOI: 10.1007/978-3-540-45215-7_2

[9] Information risk analysis methodology (IRAM), Information Security Forum (ISF), Available at: https://www.securityforum.org/iram

[10] Virtual Data Centre (VDC) – A New Concept in Service Delivery, BT, Available at http://globalservices.bt.com/LeafAction.do?Record= Virtual_Data_Centre_products_uk_en-gbLast Accessed November 2010

[11] I. Foster, Y. Zhao, I. Raicu, S Lu. Cloud Computing and Grid Computing 360-Degree Compared. In GCE '08: Grid Computing Environments Workshop, pages 1–10. IEEE, November 2008

[12] P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, October 2009

[13] R. Buyya, K. Bubendorfer. "Market Oriented Grid and Utility Computing", Wiley Press, New York, USA, 2008.

[14] R. Sailer, T. Jaeger, E. Valdez, Building a MAC-Based Security Architecture for the Xen Open-Source Hypervisor. Proceeding ACSAC '05 Proceedings of the 21st Annual Computer Security Applications Conference

[15] Vmwarenat networking buffer overflow vulnerability. [Online]. Available: http://secunia.com/advisories/18162/

[16] M. Carpenter, T. Liston, and E. Skoudis, Hiding virtualization from attackers and malware, IEEE Security and Privacy, vol. 5, no. 3, pp. 62–65, 2007

[17] C. Cifuentes, A. Fraboulet, Intra procedural static slicing of binary executables, Proceedings of the International Conference on Software Maintenance, Bari, Italy, Oct 1997, pages 188–195, IEEE-CS Press

[18] J. Bergeron, M. Debbabi, J. Desharnais, M. M. Erhioui, Y. Lavoie, N. Tawbi, Static detection of malicious code in executable programs, Int. J. of Req. Eng. (2001)

[19] P. Saripalli and B. Walters, QUIRC: A Quantitative Impact and Risk assessment framework for Cloud security, pgs:280-288, Proceedings of IEEE 3rd International Conference on Cloud Computing, 2010

[20] SAS 70 Type 2 Audit, SAS 70, Website Available at http://sas70.com/sas70_overview.html

[21] U. Bayer, A. Moser, C. Kruegel, E. Kirda, Dynamic Analysis of

Malicious Code, EICAR 2006 Special Issue

[22] Afnan Ullah Khan1,2, Manuel Oriol2,3, Mariam Kiran, Ming Jiang, Karim Djemame," Security Risks and their Management in Cloud Computing"IEEE,2012