ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Designing a Framework for Detection and Capturing of Network attacks in Cloud Computing: a Literature Review

Mukul Pande [1], Prof. Sulabha Patil [2]

P.G. Student, Dept. of Computer Engineering, Tulsiramji Gaikwad-Patil College of Engg. & Tech., Nagpur, India[1]

Professor, Dept. of Computer Engineering, Tulsiramji Gaikwad-Patil College of Engg. & Tech., Nagpur, India[2]

ABSTRACT: With the advent of the new developments in cloud computing, it has proven a cure for ever increasing thirst to expand computational infrastructure, with the increase in PAAS and IAAS scalability, and on demand computing the sector proves economical for business and also for the service provider. But with the new tech coming in like CDN and other layers of abstraction the business hosting the software/ service has very less know how about the actual location and the other forensic data , and has to rely on the third party solutions for monitoring the servers / VPS in our case. The system is reactive in nature and in case of any event the cloud provider will assess the situation and act on it, the end user won't even know about the event as the fail-overs and backups will kick in. We are suggesting a system which will reside on the server application or the host operating system and allow to silently monitor the health and other parameter's of the system that are not available to the service company's system analyst and share the complete health log and also provide additional data to the remote server where in a web based control panel will be provided to monitor all the hosts at the same time. This will help the service company to monitor heterogeneous server architecture over different regional boundaries with a unified system along with all the logs and forensic data at regular interval or on demand. This will also help the service availing company to be in some control over the policy of the data and also monitor the events occurring in the cloud with the time stamp to recreate the scenario, this will specially benefit the distributed environment and CDN networks as this will re-register the same server according to replication for CDN networks load balancers.

KEYWORDS: IAAS, Load balancer, CDS, network.

I. INTRODUCTION

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new communications, training new workforce, or authorized new software. It extends Information Technology's (IT) existing. The survey is based on the following points.

1. The paper aims to overcome the basic problem of obtaining additional forensic information of a virtual machine or a container provided by the cloud provider and in case of attack report the same to a third party security provider for further action.

2. The Cloud provider often deploy high availability cluster configuration to provide maximum availability for the service provided and nowadays with the advent of the CDN (Content Delivery Network) the network has undergone additional layers of abstraction which is governed by the cloud service providers. Critical information such as IP, Physical Location of data and other network parameters.

3. The paper aims to provide a client server system which when installed in the cloud environment will be able to detect all the essential parameters and report to a remote server or service for further analysis and action .

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

II. OBSERVATIONS OF RELATED WORK

In this paper by Balachandra Reddy Kandukuri Ramakrishna Paturi V & Dr. Atanu Rakshit [1] have focused on the security issues related to data in the cloud computing, where the vendor has to provide some assurance in service level agreements (SLA) to convince the customer on security issues. Cloud is provided as Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Each service has its own security issues. So the SLA has to describe different levels of security and their complexity based on the services to make the customer understand the security policies that are being implemented and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. In this paper, they put forward some security issues that have to be included in SLA.

Wesam Dawoud, Ibrahim Takouna, Christoph Meinel [2] has discuss an elaborated study of IaaS components' security and determines vulnerabilities and counter measures. This paper proposed a Security Model for IaaS (SMI) to guide security assessment and enhancement in IaaS layer. Cloud Computing represents a new computing model that poses many demanding security issues at all levels, e.g., network, host, application, and data levels. The variety of the delivery models presents different security challenges depending on the model and consumers' Quality of Service (QoS) requirements. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer.

Victor Echeverr´ıa, Lorie M. Liebrock, and Dongwan Shinm [3] says one of the challenging problems cloud computing is facing today is the security of data in the cloud. In this paper, the authors discuss a novel approach to controlling access to user data in the cloud; the concept is called Permission as a Service (PaaS). Specifically, PaaS separates access control from other services to provide a separate service in the cloud. This allows users to set permissions for all data in a single location. In PaaS, user data are encrypted to maintain confidentiality and permissions are managed via decryption keys. As a proof-of-concept, the author had discussed the design and implementation of our prototype leveraging attribute based encryption (ABE).

Jianfeng Yang Zhibin Chen [4] analyzed that Cloud computing is a rapidly developing information technology, has aroused the concern of the whole world. Cloud computing is Internet-based computing, whereby shared resources, software and information, are provided to computers and devices on-demand, like the electricity grid Cloud computing is the product of the fusion of traditional computing technology and network technology like grid computing, distributed computing parallel computing and so on. It aims to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing entity, and using the advanced business models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to distribute the powerful computing capacity to end users' hands. This article introduces the background and service model of cloud computing. This article also introduces the existing issues in cloud computing such as security, privacy, reliability and so on. Proposition of solution for these issues has been provided also.

According to Mohemed Almorsy, John Grundy and Amani S. Ibrahim [6] cloud computing model is considered to be a very promising internet-based computing platform, it results in a loss of security control over the cloud-hosted assets. This is due to the outsourcing of enterprise IT assets hosted on third-party cloud computing platforms. Moreover, the lack of security constraints in the Service Level Agreements between the cloud providers and consumers results in a loss of trust as well. Obtaining a security certificate such as ISO 27000 or NIST-FISMA would help cloud providers improve consumers trust in their cloud platforms' security. However, such standards are still far from covering the full complexity of the cloud computing model. The author had introduce a new cloud security management framework based on aligning the FISMA standard to fit with the cloud computing model, enabling cloud providers and consumers to be security certified. This framework is based on improving collaboration between cloud providers, service providers

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

and service consumers in managing the security of the cloud platform and the hosted services. It is built on top of a number of security standards that assist in automating the security management process. The authors have developed a proof of concept of our framework using .NET and deployed it on a test bed cloud platform. The authors evaluated the framework by managing the security of a multitenant SaaS application.

Jean-Paul Smets-Solanes, Christophe and Romain Courteaud [8] has discussed SlapOS which is an open source grid operating system for distributed cloud computing based on the moto everything is a process. SlapOS combines grid computing and Enterprise Resource Modeling (ERP) to provide Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) through a simple, unified API which one can learn in a matter of minutes. Due to its unified approach and modular architecture, SlapOS has been used as a research testbed to benchmark No SQL databases and optimize process allocation over intercontinental Cloud. SlapOS opens new perspectives for research in the area of resilience and security on the Cloud.

NM Karie, HS Venter [6] have focused on ontological framework meant to provide a structure and depiction of the different cloud environments and components an investigator should be acquainted with, in the case of a cloud investigation process. In addition, the relationships and interactions between the different environments by capturing their content and boundaries are also shown in this paper regarding the security area of cloud computing. Furthermore, the purpose of this paper is meant to provide a common ontological framework for sharing coherent cloud computing concepts and also promote the understanding of the cloud environments and cloud components regarding to Cloud Forensics.

Lori M. Kaufman, Lori Kaufman & Bruce Potter [5] had presented a set of recommended restrictions and audits to facilitate cloud security. Although the recommendations might be overkill for deployments involving no sensitive data, they might be insufficient to allow certain information to be hosted in any public or community cloud.

Farzad Sabahi[10] has summarized reliability, availability, and security issues for cloud computing (RAS issues), and propose feasible and available solutions for some of them. The author have discussed Gartner's seven security issues such as Privileged user access, data location recovery etc. They have also explained cloud RAS issues such as data leakage, cloud security issues etc.

Ralf Teckelmann and Christoph Reich [15] analyzed the idea behind cloud computing is to deliver Infrastructure-, Platform- and Software-as-a-Service (IaaS, PaaS and SaaS) over the Internet on an easy pay-per-use business model. However, current offerings from cloud providers are based on proprietary technologies. As a consequence, consumers run into a risk of a vendor lock-in with little flexibility in moving their services to other providers. This can hinder the advancement of cloud computing to small- and medium-sized enterprises. To address these issues, standardization efforts have to take place in order to support further developments in the clouds. Standardized exchange mechanisms and interfaces are crucial in order to facilitate interoperability. In this paper, the author looks at several cloud standards, such as Open Virtualization Format, Open Cloud Computing Interface, and Cloud Data Management Interface, and analyzes them against a taxonomy in order to point out their role for interoperability in IaaS. The taxonomy presents important IaaS topics, such as access mechanism, virtual appliance, security, and service-level agreement

Farhan Bashir Shaikh & Sajjad Haider [12] has discussed their observations of security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing. This work will enable researchers and security professionals to know about users and vendors concerns and critical analysis about the different security models and tools proposed. Which will help to find the solution to the query such as How the end users of cloud computing know that their information is not having any availability and security issues? Every one poses, Is their information secure?

Volker Fusenig and Ayush Sharma [11] focused on a new approach called cloud networking which adds networking functionalities to cloud computing and enables dynamic and flexible placement of virtual resources

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

crossing provider borders. This allows various kinds of optimization, e.g., reducing latency or network load. However ,this approach introduces new security challenges. This paper presents a security architecture that enables a user of cloud networking to define security requirements and enforce them in the cloud networking infrastructure.

Wentao Liu [7] had introduces some cloud computing systems and analyzes cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system.

Zhang Xin, Lai Song-qing & Liu Nai-wen [9] have discussed the analyzed work on new security challenges which have not been taken into account completely in the current cloud computing system. They have discussed security issues on different cloud layers. As a consequence, to build a cloud computing data security system is the basis to build cloud computing security system. In this article, the cloud computing technology architecture and the cloud computing data security features are the first to be studied and considered, then the cloud computing data security model is raised. At last, the realization of data security model has been researched. The model adopts a multi-dimension architecture of three layers defence. First of all, user authentication is required to ensure that user data cannot be tampered. Users who pass the authentication can get relative operation on the user data, such as addition, modification, deletion. If the unauthorized user use illegal means to deceive the authentication system, the file entered the system encrypt and privacy defence levels. In this layer, user data is encrypted. If key has been got by the intruder. The user data cannot be got valid information even it is obtained through function of privacy protection. It is very important for commercial users of the cloud computing to protect their business secrets. The last is the file quick regeneration layer, user data can get maximum regeneration even it is damaged through rapid regeneration algorithm in this layer. Each layer accomplishes its own job and combines with others to ensure data security in the cloud computing.

Anas BOUAYAD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI [17] have discussed various security problem which had becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy, elasticity, and layers dependency stack. In this paper author had introduce a detailed analysis of the cloud security problem. They have investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders' perspective, and the cloud service delivery models perspective. Based on this analysis we derive a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution

Joel Gibson, Robin Rondeau, Darren Eveleigh and Qing Tan [13] have helped in understanding the cloud service models which are critical in determining if cloud services or hosting are an appropriate business solution, and if so, which model best balances the level of control required versus reduced hardware, configuration, and maintenance costs. Cloud computing offers many benefits to organizations; it has enabled collaboration amongst disparate communities and workgroups, and has overcome challenges that have plagued existing business solutions. However, the security, privacy, and integrity of the cloud are of prime importance and there are many challenges that exist. At the present time there seems to be a lot of momentum behind the adoption of cloud computing despite these. This may simply be a trend, an indication that society truly wants their data to be available whenever from anywhere, or a sign that few understand the associated risks.

Gansen Zhao,Ziliu Li, Wenjun Li Hao Zhang Yong Tang[18] have shared their observations that using a cloud service for a user has no privilege in managing the underlying computing platform nor the underlying resource and infrastructure, leading to the situation that a user has no way to monitor cloud services' behaviour to protect the user's privacy. They have proposed a privacy enhancing framework on PaaS for detecting the privacy violating behaviour and protecting user's information instantly by enforcing related protection actions. The proposed framework

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

allows customized security policies and behaviour analysis models, enabling users to impose application oriented privacy monitoring mechanisms.

Alberto da Silva, Anderson Soares Ferreira Campinas, & Paulo Licio de Geus[14] have shared their views on the recent literature in the field prioritizes the administration of resource provisioning and the allocation algorithms for an energy-efficient management of cloud computing environments. Security metrics can be seen as tools for providing information about the security status of a certain environment. With that in mind, we tackle the management of cloud computing security by using GQM methodology to develop a cloud computing security metrics hierarchy. The main goal of their proposed hierarchy is to produce a security index that describes the security level accomplished by an evaluated cloud computing environment. In a second step, this security index is used to compute an allocation index that helps in setting management priorities with a security bias. We also present a methodology for cloud computing management using security as a criterion.

Keiko Hashizume, Eduardo B. Fernandez, Maria M. Larrondo-Petrie [23] have discussed the three primary types of cloud computing services are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). IaaS delivers computer infrastructure including servers, storage and network. PaaS offers the computer platform as a service which facilitates development and deployment of applications. In SaaS, applications are hosted and maintained by a cloud provider and delivered to the users as services on demand. They have developed two patterns for cloud delivery services: IaaS and PaaS patterns. They developed here a pattern for Software-as-a-Service to complete all the three cloud service levels. These patterns will be used to study cloud security requirements.

Josiah Dykstra and Alan T. Sherman, Cyber Defense Lab, Department of CSEE [16], have emphasized on the model to show the layers of trust required in the cloud. Secondly, they have presented the overarching context for a cloud forensic exam and analyze choices available to an examiner. Also for the first time they have proposed an evaluation of popular forensic acquisition tools including Guidance EnCase and Acces Data Forensic Toolkit, and shown that they can successfully return volatile and non-volatile data from the cloud

Farzad Sabahi, *Member, IEEE*, [22] have focused on new security architecture in a hypervisor-based virtualization technology in order to secure the cloud environment virtualization technology is built on virtualization technology which is an old technology and has had security issues that must be addressed before cloud technology is affected by them. The paper also emphasizes on relation between reliability and security in virtualization, virtual machines security threats and attacks in virtualization

Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd[19], have identified a cross-disciplinary approach between cloud forensics, digital forensics and cloud Computing. This paper has also shown the role trusted third parties and the cloud service providers' perspectives and has explained whether they can gain the authority to get access to the evidence. And finally, for service providers' point of view this paper has summarized whether they able to guarantee the safety of the data.

Ashalatha R [21] has provided a comprehensive review on the essentiality of Security- as- Service in cloud computing scenario. The paper also presents the significance of data security and the various existing security techniques for the cloud. This paper also focus on security issues encountered in cloud computing.

Chiang Ku Fan and Tien-Chun Chen, Shih Chien University [20] have focused on "Cross-Cloud Compatibility. The findings also revealed that people who work in the field of information or Cloud Computing are somehow ignorant of where the risks in Cloud Computing lie due to its novelty and complication. The major contribution of this paper lies in the identification and verification of Cloud Computing services' risk factors.

Mohsen M. Doroodchi, Amjad Ali [24] examined the forensics as a scientific discipline, in addition to the traditional view, and analyzes the past and future trends of its models. Furthermore, key characteristics of a framework for next generation uniform models that are adaptable to computer science discipline are identified. The proposed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

model in this paper incorporated certain features of the past models to provide a new framework. In particular, the ontology of current computer technology in addition to abstraction layers of forensic science used to provide the structure of this model.

George SIBIYA, Hein S. VENTER and Thomas FOGWILL [25], have examined a framework aimed at addressing digital forensics challenges in a cloud environment. The framework addresses the issue of data acquisition in the cloud that may be beyond the jurisdiction of investigators. It makes use of accessible information to build up a case before the costly data acquisition from foreign countries could be carried out.

III. PROPOSED METHODOLOGY

In this proposed scheme focus is given on security in cloud therefore implementing a framework for detection and capturing of network attacks in cloud computing where first step is to implement window's service to boot on start up and, gather data required for the project, (ip, hostname, ports status), further post request to the server for logging data. Analyzing vulnerabilities in the cloud and detecting network attacks in virtualized environment recreate the common two scenarios ddos, and brute force attack for application access in cloud environment. Then setup a web based server with asynchronous connections to all the clients for logging data. Then design and implement a user interface for the admin to monitor abnormalities in the clients log the type of attacks on the system and suggest action to be taken. Setup a private cloud and simulate the project along with two network attacks on the system. Log data over the network and analyze the output. Setup distributed scenarios with a standalone system, along with public cloud and a private cloud to study the system behaviors in real scenarios .Integrate complete system to log data centrally and render final UI and software package.

IV. CONCLUSION

Cloud Computing is in a period of strong growth, but this technology still has some issues of security and somewhat it is immature. This paper highlights many of the security issues in the cloud computing environment at different levels of infrastructure and cloud layers. We provide a definition of cloud computing forensics to scope this area. We discuss various cloud layers, services security and their roles. We examined recent research papers and involved the international community. Our categories of challenges include architecture, data collection, analysis, anti-forensics, incident first responders, role management, legal issues, standards, and training.

The project aims to overcome the basic problem of obtaining additional forensic information of a virtual machine or a container provided by the cloud provider and in case of attack report the same to a third party security provider for further action.

In this paper, we have discussed the issues related to data location, storage, security, availability and integrity. Establishing trust is the way to overcome these security issues as it establishes entities relationship quickly and safely. For this purpose, we have surveyed some of the trust management models. Since trust is an abstract and subjective term; hence, it is difficult to measure and manage the trust.

REFERENCES

1) Balachandra Reddy Kandukuri ,Ramakrishna Paturi ,Dr. Atanu Rakshit "**Cloud Security Issues"** © IEEE DOI 10.1109/SCC.2009.84, 978-0-7695-3811-2/09, 2009.
2) Wesam Dawoud, Ibrahim Takouna, Christoph Meinel, "Infrastructure as a Service Security: Challenges and Solutions" 4IDC Enterprise Panel, August 2008.
3) Victor Echeverr´ıa, Lorie M. Liebrock, and Dongwan Shin "Permission Management System: Permission as a Service in Cloud Computing" 34th Annual IEEE Computer Software and Applications Conference Workshops, 2010.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

4) Jianfeng Yang Zhibin , "Cloud Computing Research and Security Issues" IEEE, 978-1-4244-5392-4/10 ©2010.
5) Lori M. Kaufman, lori.kaufman@ieee.org Bruce Potter, "Monitoring Cloud Computing by Layer".
6) Mohemed Almorsy, John Grundy and Amani S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework", IEEE DOI 10.1109/CLOUD.2011.9, 978-0-7695-4460-1/11 $26.00 © 2011.
7) Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", IEEE, 978-1-4577-1415-3/12/$26.00 ©2012.
8) Jean-Paul Smets-Solanes, Christophe C´eriny and Romain Courteaud, "SlapOS: A Multi-purpose Distributed Cloud Operating System Based on an ERP Billing Model", IEEE International Conference on Services Computing, DOI 10.1109/SCC.2011.97, 978-0-7695-4462-5/11 © 2011.
9) Zhang Xin, Lai Song-qing, Liu Nai-wen, "Research on Cloud Computing Data Security Model Based on Multi-dimension". INTERNATIONAL SYMPOSIUM ON INFORMATION TECHNOLOGY IN MEDICINE AND EDUCATION, 978-1-4673-2108-2112 ©2012 IEEE
10) Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE 978-1-61284-486-2/111$26.00 ©2011.
11) Volker Fusenig and Ayush Sharma, "Security Architecture for Cloud Networking", IEEE, 978-1-4673-0009-4/12/$26.00 ©2012.
12) Farhan Bashir Shaikh & Sajjad Haider "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions", IEEE, 11-14 December 2011, Abu Dhabi, United Arab Emirates978-1-908320-00-1/11/$26.00 ©2011.
13) Joel Gibson, Robin Rondeau, Darren Eveleigh, *Qing Tan* "Benefits and Challenges of Three Cloud Computing Service Models", IEEE, 978-1-4673-4794-5/12/$31.00_c 2012.
14) Criteria Carlos, Alberto da Silva, Anderson Soares, Ferreira Campinas, Brazil, Paulo Licio de Geus "A Methodology for Management of CloudComputing using Security", IEEE, 978-1-4673-5163-8/12/$31.00 © 2012.
15) Ralf Teckelmann and Christoph Reich "Mapping of Cloud Standards to the Taxonomy of Interoperability in IaaS", Department of Computer Science Hochschule Furtwangen University, Germany Email: {ralf.teckelmann, rch}@hs-furtwangen.de Anthony Sulistio, IEEE DOI 10.1109/CloudCom.2011.78, 978-0-7695-4622-3/11 $26.00 © 2011.
16) Josiah Dykstra and Alan T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques", Cyber Defense Lab, Department of CSEE University of Maryland, Baltimore County (UMBC) 1000 Hilltop Circle, Baltimore, MD 21250 April 18, 2012
17) Anas BOUAYAD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI, "Cloud computing : security challenges", IEEE, 978-1-4673-2725-1/12/$31.00 ©2012.
18) 2012 International Conference on Cloud Computing and Service Computing Privacy Enhancing Framework on PaaS Gansen ZhaoSchool of Computer Science South China Normal University Guangzhou, China Ziliu Li, Wenjun Li School of SoftwareSun Yat-Sen University Guangzhou, China Hao Zhang Jiesai Co. Ltd Guangzhou, China Yong Tang School of Computer Science South China Normal University Guangzhou, China 978-0-7695-4910-1/12 $26.00 © 2012 IEEE DOI 10.1109/CSC.2012.27[18]
19) Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, "A Survey on Cloud Computing and Digital Forensics", Journal of Next Generation Information Technology (JNIT) Volume4, Number6, August 2013.
20) Chiang Ku Fan and Tien-Chun Chen, Shih Chien University, " The Risk Management Strategy of Applying Cloud Computing" , (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 9, 2012
21) Ashalatha R, "SURVEY ON SECURITY AS A CHALLENGE IN CLOUD COMPUTING", International Journal of Advanced Technology & Engineering Research (IJATER) National Conference on Emerging Trends in Technology (NCET-Tech)
22) Farzad Sabahi, Member, IEEE, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012.
23) Keiko Hashizume, Eduardo B. Fernandez, Maria M. Larrondo-Petrie, "A pattern for Software-as-a-Service in Clouds", (Cyber Security 2012) / 2012 ASE International Conference on BioMedical 978-0-7695-4938-5/12 © 2012 IEEE DOI 10.1109/SocialInformatics.2012.106
24) Mohsen M. Doroodchi, Amjad Ali, " Framework for Next Generation Digital Forensics Models", Center for Security Studies, University of Maryland University College, Adelphi, Maryland, USA
25) George SIBIYA, Hein S. VENTER and Thomas FOGWILL, "Digital Forensic Framework for a Cloud Environment", *IST-Africa 2012 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, 2012 ISBN: 978-1-905824-34-2*