GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

AN ANALYTICAL OF RESEARCH METHODOLOGY ON SURVEY OF CLOUD TECHNOLOGY WITH SECURITY

[*1]Royyuru Srikanth & [2]Dr S M Tiwari
[*1]Research Scholar, Department of CSE, University of C S M Kanpur
[2]Professor in CSE Department of CSE, University of C S M Kanpur

ABSTRACT

Cloud computing is a developmental consequence of previous IT approaches based on existing and new technologies. Cloud computing is a model of on-demand network access to a shared pool of resources such as servers, storage, applications and related services. Cloud computing can be offered and published with minimal interaction and preferably without the intervention of the cloud service provider. By increasing the awareness and implementation of cloud services and underlying technologies, security requirements are up-to-date. These developments have created new security issues, including security issues that are still growing. This document provides an overview and study of cloud computing, with various security risks, security problems, currently used cloud technologies and countermeasures. Security challenges in cloud computing are huge, especially for public clouds whose infrastructure and computer resources are owned by an outsider who sells these services to the public. Security requirements in the cloud have been addressed in previous publications, but it is still difficult to estimate which types of requirements have been studied and are still poorly studied. This document performs a systematic review of the literature by identifying the security requirements of cloud computing from publications. In addition to security issues, the positive side of information security in cloud computing has also been part of this work

Keywords: Security. Cloud Technology, Computing, Service Modulization.

I. INTRODUCTION

The first project to define cloud computing was created in November 2009. After years of work and 15 projects, the operational definition of cloud computing from the National Institute of Standards and Technology (NIST), the 16th and final definition NIST Definition of Cloud Computing (NIST Special Publication 800-145). According to the official definition of NIST, "cloud computing is a model for accessing the ubiquitous, convenient, on-demand network from a shared pool of configurable computer resources (networks, servers, storage, applications, and services)." Cloud computing is generally supported due to the fact that virtualisation or multitenancy is the required cloud functionality, but it is cloud computing, which is more popular because of facts that have contributed to lower prices and easy implementation for the pay per use model. attracted attention and becoming increasingly popular due to lower capital expenditures and operating costs General examples of cloud services are Google Apps, Oracle Cloud, Microsoft Office 365, etc.In the rest of this research paper, the term cloud refers to the term cloud computing. A cloud provides a cloud service user (CSU) with privileged access to an application, platform or infrastructure "as a service" [1]. CSU uses the service of the Cloud Service Provider (CSP).

The National Institute for Standardization and Technology (NIST) in the United States has defined three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service. that service (IaaS). It is also the most important SPI service model. A new term that is not defined by NIST but is becoming increasingly popular in newsletters and conferences, is XaaS, a collective term that applies to many things, including 'X as a service'. "," everything as a service "or" everything as a service. "NIST has also defined four types of implementation models: private, community, public and hybrid models, and the security of information in the cloud depends on this different level of control in different service models and implementations In various investigations and investigations, including that of the International Data Corporation (IDC), security is the main challenge or obstacle to the application of cloud computing technologies in various sectors of the industry .The rapid growth of cloud computing has many security problems delivered to users and suppliers of cloud services, which is the main reason to deepen this area and to investigate the likely threats to adoptability and to provide a review of the literature on important issues.The main goal of this research paper is the public implementation of the cloud, because there are more security aspects are required in this implementation model.

Problem: in recent years research has been conducted into cloud computing and security. Adoption is increasing, but not at the same pace in all segments of the industry, such as healthcare; this requires more in-depth information about the latest cloud security threats and related solutions. The purpose of this article is to prepare a more thorough and structured overview of information security requirements in the cloud and the proposed solution to these requirements. This paper also focuses on what is most widely published in empirical studies and what is still needed to deepen.

Research question: The following research questions were addressed in this research paper.
RQ1: What are the main information security issues and measures that are generally addressed in most publications?
RQ2: There are improvements in the field of information security in cloud computing.
RQ3: Which security problem with the cloud is most desirable?

1.2. Research Methodology.

A systematic review of the literature was conducted to answer the above research questions. Because cloud computing has become more popular in recent years, no restriction on the year of publication has been taken into account. We have considered a number of limitations: the studies included in the selected sources must be written in English and these sources must be available on the internet. Science Direct, ACM Digital Library, IEEE Digital Library and Google Scholar were considered as tools. A first investigation into cloud computing and security issues was completed and a total of 97 documents were collected. In order to focus on the most relevant literature, security problems were discussed as mentioned in the cloud. The safety guidelines of the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance (CSA) have been taken into consideration. A primary evaluation was performed based on the reading of abstracts of all selected articles. The inclusion and exclusion criteria for this study were based on the research question mentioned above. Some of the references mentioned in the literature in the aforementioned sources have also been considered. There is other related work, since several researchers have studied the field of cloud computing and the problems and challenges, this paper focuses on topics / issues that are now more studied and that miss research efforts for the mentioned goals.

II. DISCUSSION ON THE SAFETY OF INFORMATION IN THE CALCULATION OF THE CLOUD.

The selected literature will now be evaluated on the common problems in the NIST and CSA guidelines. This literature study also helps us to identify areas that are more in demand than other problems and that require further research. This will help us to determine recommendations for future work and research.

2.1. Data management

It is worth noting that potential providers of cloud services would have security concerns regarding the storage and processing of sensitive data [8]. The data is displayed in the following states.

Residual data: - Residual data refers to all data in the memory of the computer and relates to the data stored in the CSP file. In the case of the cloud, because the data is stored in the provider's memory and has more control than in the client. Therefore, it is necessary to ensure that CSP meets the standard security rules and that the data centre of the service provider is certified for at least the type of customer activity. If the client is a health professional, the data centre must be HIPPA-compliant and if the client is a bank, the CSP data centre must be compatible with PCI-DSS, and so on. [8]

Moving data: - Mobile data refers to data when they are moved from one stored status to the same or another module at a different location. Mobile data can also refer to data in the transition and do not necessarily have to be permanently stored. In addition, the user name and password for accessing the website are also additional data on the road. [8] Problems with data management are discussed below.

Data issues: To illustrate the potential magnitude of this threat, CSA referred to a research paper on how a virtual machine could use side channel synchronization data to extract personal cryptographic keys [4] [5]] from other virtual machines on the same server. If a multi-tenant hosted cloud service database is not designed correctly, a single error in a client application can allow a malicious user to obtain not only the data from that client, but also the data from each client. other customer.
Loss of data and losses: - Data loss occurs when data is in the wrong hands, at rest, in motion or in progress. Identify data loss prevention (DLP) solutions and prevent unauthorized attempts to copy or transmit sensitive data, deliberately and / or unconsciously, without permission, by individuals who have access to sensitive information

[12]. Detect DLP solutions and prevent unauthorized attempts to copy or transmit sensitive data, deliberately and / or unconsciously, without permission, by persons authorized to access sensitive information.

The cleaning data: - data cleaning is the removal of sensitive data from a storage device in different situations, for example when a storage device is removed from operation or stored in a different way. Data cleanup also applies to the backup copy that was created to restore services under certain conditions. Because the data can only be completely removed from the media if the device is destroyed, attackers may be able to recover data from the replaced media for maintenance or other reasons. [11]

Data backup: - Data backup is an important aspect to enable disaster recovery, but in the case of cloud computing it can introduce security issues [3]. Sometimes cloud providers outsource backup to external service providers, which can lead to other legal problems.

Data Lock in: - The data is stored by the service provider in its own CSP format and can not easily be exported or modified for a new environment. [8] The cloud service user must prevent data from being blocked and discussed in detail with CSP before this technology is applied.

Ownership of data: - The ownership rights of the organization above the data must be firmly established in the service contract [1]. Intellectual property, including original works created using the cloud infrastructure, can be archived. The cloud customer must ensure that the contract respects as far as possible the rights to intellectual property or original work, without compromising the quality of the service offered [7]. Cloud Service The user must also check the status of his metadata. Metadata is simply data about the data.

Location of data: - When information is cross-border, legal, privacy and regulatory systems can be ambiguous and raise many concerns. One of the problems that must be solved, one might wonder whether the laws of the country in which the data are collected, so the flow, regardless of whether these laws continue to apply to post-data transfer and or laws add extra risks or benefits. Technical, physical and administrative security measures, such as access controls, are often used. Acts and regulations - The FISMA requires federal agencies to adequately protect their information and information systems against unauthorized access, use, disclosure, disruption, alteration or unauthorized destruction; This is mandatory if the data is managed by the agency or its contracting third party. There are a number ofindustry-specific standards such as Health Insurance Portability and Accountability Law (HIPAA) and Payment Data Industry Standard (PCI DSS). [1] Measure data management: - The cloud service providers become more sensitive to legal and regulatory issues and may be willing to store and process in certain jurisdictions and implement security and security protections. privacy. However, it remains to be seen to what extent they accept the responsibility to put the content under their management. Even then, organizations are responsible for the security and privacy of data held on their behalf by a cloud service provider. These problems occur mainly because of sufficient due diligence. It is recommended that the CSU has sufficient resources to carry out appropriate due diligence before going to the cloud. Simple text developed over time can contain important documents about users. CSU can request the confidentiality of its metadata and the destruction of such information permanently after termination of the contract.

2.2. Traffic control service

If an attacker has access to your credentials, he can intercept your operations and transactions, manipulate data, return modified / incorrect information, and redirect your customers to unwanted sites. Account or service instances can become a new foundation for the attacker. From there they can use the power of your reputation to carry out subsequent attacks. [21] Countermeasures: - Organizations should try to prohibit the sharing of account credentials between users and services and, if possible, to use two-factor authentication techniques. The Cloud Security Alliance (CSA) has published a guide on identity and access management with a list of recommended best practices for disciplinary action. [12].

2.3. Unsafe interfaces and APIs

System administrators rely on interfaces and Application Program Interface (API) for cloud provisioning, management, orchestration and monitoring. Often, organizations and third parties known to be able to build on these interfaces are injecting additional services to enable system management. Weak interfaces and APIs can expose an organization to these security issues related to privacy, integrity, availability and liability [6].

Countermeasures: Organizations, especially orchestration layer developers and cloud domain providers, need to understand the security implications of using, managing, orchestrating and monitoring cloud services and embrace necessary steps during the development of these interfaces and APIs [6]

2.4. Denial of Service Attack

The DoS has been a major threat for years, but it is a potential threat to the CSP and CSU. An attacker can use as many Cloud Client resources as possible and the system cannot meet requests from other legitimate users due to unavailable resources. DoS interrupts [20] may cost service providers, customers, and customers that are billed based on processing cycles, bandwidth, and disk space.When the bandwidth is high and the enhanced security features implemented by the CSP, an attacker may not be able to eliminate a service, but may still consume a lot of time and use the service. bandwidth Because CSUs are billed using the cover model for resources such as the calculation cycle, storage and bandwidth, and so on. In these cases, it becomes too expensive for CSU and you should do it alone.Countermeasure: - Before selecting CSP, the user must ask the network architecture questions that are available from the provider. Some ISPs offer internet bandwidth that is protected by DDOS [24]; and CSP has implemented appropriate security measures at the gateway level that protect against undesired use of Internet bandwidth and protect against DOS attacks. This can help to reduce costs and unwanted interruptions.

2.5. Insidious attacks.

Malicious insiders can be current or former employees, an entrepreneur or an external third party that uses a network, system or data for malicious purposes. These attacks are important enough for all three Cloud Computing service models, such as IaaS, PaaS and SaaS. Although cryptography is implemented and keys are not stored with the CSU and are only available when the data is used, the system remains vulnerable to malicious internal attacks. Countermeasure: Fog computing [13] that suggests that profiling user behaviour and crawling information such as honeypots can be implemented to prevent malicious insider attacks.

2.6. Cloud abuse

A legitimate hacker can use cloud servers that are hosted on the same third-party CSP or CSP to start a DDoS attack, spread malware, botnets, and so on. [10] Botnets were used to send spam, collect logon credentials and launch injection attacks against websites. Botnets can also be used to perform a denial-of-service attack against the infrastructure of a cloud provider. The hacker can enable cloud services to start phishing attacks, malware, etc. This leads to a new challenge for CSP to define what is abusive and to identify the best processes to identify it. [22]

Countermeasures: some solutions have been proposed by researchers such as burglary prevention system, network traffic, logging and some non-technical measures such as acceptable usage policy, account verification, etc. [23]

2.7. Multiple rentals

In the Cloud Computing environment, CSP shares infrastructure, platforms and applications to provide services in a scalable way. The threat of shared vulnerabilities exists in all models for cloud delivery. [25]

Countermeasure: - The CSP infrastructure must be designed and implemented to provide strong insulation properties for multi-tenant architecture (IaaS), redeployment platforms (PaaS) or multi-client applications (SaaS).

2.8. Complexity of the system

A public cloud computing architecture is a bit complex compared to the internal distribution of the same service. A public cloud architecture, such as any internal solution, can include application deployment, IT infrastructure, storage, support middleware, virtualization, third-party virtual machines, and so on. But it can also include other management backgrounds, such as self-service resource allocation, quota management, metering, data replication and recovery management, and so on. The public cloud service itself may be a nested architecture provided by other cloud service providers. Security is therefore dependent on a more complex architecture.

Countermeasure: a subscriber of this service must take care of the cloud architecture according to his needs and keep all aspects in his risk assessment plan. [7]

2.9. Loss of control

Migration to a public cloud requires the transfer of control to the cloud provider; your data and other system components that were previously under the direct control of the customer. This loss of control [26] will affect the ability of the subscriber to maintain situational awareness, to find alternatives and to prioritize the most appropriate activities for the customer's organization. The loss of control differs according to three service models (SaaS, Paas, Iaas).

Countermeasure: due diligence should include the supplier solution architecture and the risk assessment should be planned accordingly.

2.10. Virtualization problems

So far, we have talked about multi-leasing, the pool of resources, etc. To achieve this goal, virtualisation of computer resources is one of the most important building blocks of Cloud Architecture. Virtualization allows users to create, copy, share, migrate and restore virtual machines, allowing them to run various applications. In Virtualization, a second logical level is added to create virtual machines. Security becomes more complex thanks to the extra layer and the complex interconnectivity [14].

Shared resources: - Virtual machines hosted on the same physical server share the CPU, memory, I / O, network, and so on. Sharing resources between virtual machines can cause security problems between different virtual machines. For example, a malicious virtual machine can derive information from other virtual machines through shared memory or other shared resources without compromising the hypervisor. VM escape, the program running on a virtual machine can completely ignore the virtual level (hypervisor level) and access the host computer.

Unchecked VM images: - In virtualization, an image of the virtual machine is a pre-packaged software model that contains the configuration files used to create new virtual machines. You can create your own image from scratch or use an image stored in the repository of the service provider. An attacker with a valid account can create an image with malicious code. If another client uses this image to create a virtual machine, the new virtual machine will be infected by the hidden malware. These images can therefore form the basis for the general protection of virtualisation [15].

Exposed IP address of virtual machines: - Network components can also be shared by different clients because of the resource pool. In virtualization, virtual networks are configured via bridging or routing in the hypervisor virtual switch. This can lead to a number of attacks, such as sniffing and spoofing the virtual network. Virtual machines have IP addresses that can be visible to everyone in the cloud and therefore the attacker can map the virtual target machine [17]

Countermeasure: virtualization problems can be solved by correctly configuring the guest / guest interaction. [14] Traditionally, firewalls are configured on gateways, but for better security measures, firewalls can be configured in the vicinity of the hypervisor for virtualization.

2.11. Compliance and governance

According to the NIST guidelines, "compliance means that a specified specification, standard, regulation or law is complied with." Different types of security and privacy laws and regulations exist in different countries at national, state and local level, ensuring compliance is potentially complex for cloud computing. "Often companies take the cloud completely without fully understanding the specific CSP cloud environment and the associated risks, for example, entering the cloud can create contractual issues with suppliers about liability and transparency, because a DSP must have a disaster recovery site in another country and the law of the country is mentioned in the contractual agreements and the law of the country of the DR site can indicate that it has access to the data stored in the data center that is distributed in their country for specific reasons. the privacy of data is at stake in the CSU.

According to the NIST guidelines for security and privacy in public cloud computing; "Governance includes monitoring and monitoring policies, procedures and standards for application development, as well as designing, implementing, testing and monitoring the implemented services." A survey of more than 900 professionals in information technology across Europe and the United States indicates that participants are worried about cloud computing services being used unconsciously in parts of their respective organizations. Ensuring that systems are safe and that risks are managed is a challenge in every environment and even more intimidating with cloud computing.

Countermeasure: - In order to manage the board, organizations / CSUs must set up a risk management program that can withstand the ever-changing risk landscape. Each implementation on CSP must be assessed by the risk management program. The UHC must have control mechanisms to determine how data is stored, protected and used, and also take into account the remaining probable threats, as discussed in this research paper.

2.12. Service level agreements

An SLA represents the agreement between the cloud subscriber and the expected service provider for cloud services and, if the provider does not provide the service at the specified level, the compensation available to the cloud subscriber. [1]

Countermeasure: - The exit clause must be indicated with the correct data transfer, data disinfection and service transposition. In case the customer wants to migrate a service to a third party service provider, the current cloud service provider must provide provisioning support, including data migration, knowledge transfer and integration, respectively.

2.13. Incident Answer

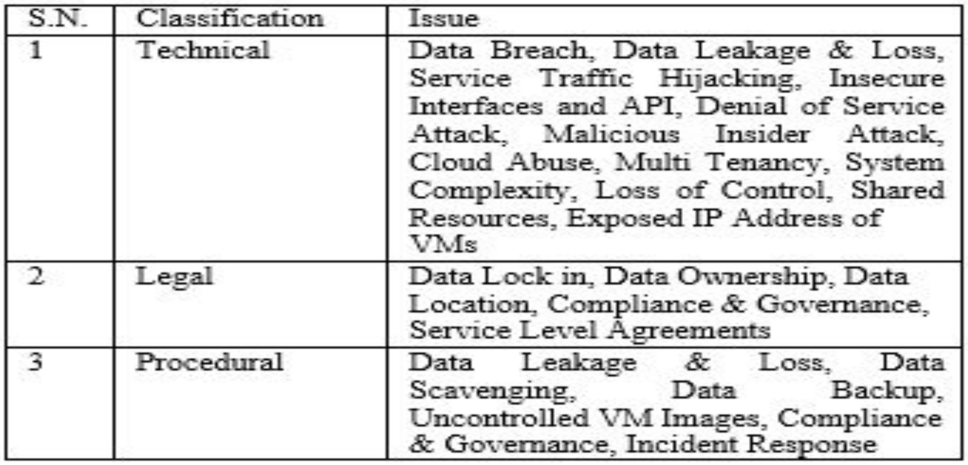
Incidental reactions mean dealing with information security incidents in an organized way. Incident management [27] includes incident reporting, incident verification, anti-rape analysis, retention (reduction of the actual incident area), collection and retention of data, improvement of problems and service reform. The response to an incident must be treated in such a way that damage is minimized and the costs of rehabilitation and other costs that may cause problems for other customers of the same payment service provider are reduced.

Resistance: the contract between CSP and CSU must include incident response and management procedures. The CSP must transparently share information with its clients during and after the incident.

III. IMPROVE THE ANALYSIS OF SAFETY ISSUES IN INFORMATION SECURITY

The problems mentioned above can generally be divided into three categories by nature, ie technical, legal or procedural. Some questions may fall into one or more categories that are classified as shown in Table 1 below.

Table: 1. Classification of Information Security Issues in cloud computing.



S.N.	Classification	Issue
1	Technical	Data Breach, Data Leakage & Loss, Service Traffic Hijacking, Insecure Interfaces and API, Denial of Service Attack, Malicious Insider Attack, Cloud Abuse, Multi Tenancy, System Complexity, Loss of Control, Shared Resources, Exposed IP Address of VMs
2	Legal	Data Lock in, Data Ownership, Data Location, Compliance & Governance, Service Level Agreements
3	Procedural	Data Leakage & Loss, Data Scavenging, Data Backup, Uncontrolled VM Images, Compliance & Governance, Incident Response

IV. IMPROVING THE SAFETY OF INFORMATION ABOUT THE COMPANY

Almost all literature on information security in cloud computing is presented as a threat, a problem, a vulnerability, a risk. On the other hand, small and medium-sized businesses can benefit from security transfers to the public cloud environment. Some of these benefits are discussed here. [1]

a) Specialization of staff: - For small organizations, with a larger scale of the computer, IT administrators must focus on tasks and other organizations that can benefit from the more experienced staff available at a cloud service provider.

b) Platform strength: - Normally the infrastructure of the service provider is kept uniform and consistent, with more patches and more hardware activities being managed than the organization's own data center. A small cloud service provider chooses to comply with the international standard HIPPA, PCI-DSS, etc.

c) Business continuity plan: - Backup and recovery policies for cloud services can be better than a small organization. The CSP provider can maintain a disaster recovery site on a remote site, which would otherwise be expensive for a small organization.

d) Orientation protection: - Security as a service is also available and time-consuming. It is difficult for smaller organizations to invest and implement the best security investments in their turn because of the costs and the lack of expertise. For example, an e-mail organization can be transferred via a cloud-based security system by directing the MX directly. Security as a service is cost-effective and useful for small organizations and is becoming increasingly more important in the field of Identity Services and Access Management, Prevention of Data Loss, Web Security, E-mail Security, Prevention and Prevention, etc.

V. CONCLUSION

Cloud computing is becoming increasingly popular because of the costs and many reasons for its users. At the same time, it could be adopted more quickly if the safety aspects are properly addressed. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture composed of a combination of different complex technologies. It is necessary to develop new security techniques to meet the cloud architecture. Security analysis was performed based on three well-known Cloud Service (SPI) models.The positive side of security in cloud computing has also been introduced; At the same time, it is advisable to be diligent before using cloud computing. We encourage the cloud service provider to teach and share the risk mitigation document with the customer. It is recommended that information security in cloud computing is not only considered a technical problem, but we must carefully plan security and privacy issues, considering legal, procedural and technical issues. This article reports on a systematic review conducted to answer three research questions that are discussed in section 1.2. The most important results of the RQ1 query are presented in part 3 of this document. The most important results of improving information security in cloud computing are also mentioned in section 4 of this document. Regarding RQ3, according to our review, cloud abuse is the most-researched security problem, followed by one of the data management problems that supports the features at the time of service migration. one supplier to another.

VI. REFERENCES

[1] Wayne Jansen Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology (NIST) Special Publication 800-144, US Department of Commerce; December 2011.

[2] E. Bangerter, D. Gullasch, and S. Krenn. Cache games: bringing access-based cache attacks on AES to practice. In 32nd IEEE Symposium on Security and Privacy;2011

[3] Subashini, S. and Kavitha, V: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34; 12011.

[4] Ziqi Wang,Rui Yang et. al: A shared memory based cross-VM side channel attacks in IaaS cloud, IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); April 2016.

[5] Arun Kumar, Dr. S.S. Tyagi, et al: "A Comparative Study of Public Key Cryptosystem based on ECC and RSA" - International Journal on Computer Science and Engineering (IJCSE), Vol 3, No. 5, pp. 1904-1905; May2011.

[6] ENISA: Cloud Computing: benefits, risks and recommendations for information Security;2009.

[7] Vic (J.R.) Winkler: Securing the Cloud Cloud Computer Security Techniques and Tactics; Jun2011

[8] Ronald L. Krutz Russell Dean Vines: Cloud Security A Comprehensive Guide to Secure Cloud Computing; July2010

[9] Yasir Ahmed Hamza, Marwan Dahar Omar: Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing. International Journal of Computational Engineering Research, Vol, 03, Issue, 6; June2013.

[10] Mather T, Kumaraswamy S, Latif S: Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc.;2009.

[11] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V3.0; 2009

[12] Salvatore J. Stolfo et al. Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. IEEE CS Security and Privacy Workshops; 2012.

[13] Reuben JS: A survey on virtual machine Security. Seminar on Network Security; Technical report, Helsinki

University of Technology; October2007

[14] *Wei J, Zhang X, Ammons G, Bala V, Ning P: Managing Security of virtual machine images in a Cloud environment. In Proceedings of the 2009 ACM workshop on Cloud Computing Security NY, USA, p 91–96;2009.*

[15] *Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D: managing Security in the trusted virtual datacenter. SIGOPS Oper. Syst. Rev. 42(1):40– 47;2008,*

[16] *Ristenpart T, Tromer E, Shacham H, Savage S: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In ACM conference on Computer and communications security, Chicago, Illinois, USA. P 199-212; 2009.*

[17] *Zhang, Y. & Joshi, :, Access Control and Trust Management for Emerging Multidomain Environments. Annals of Emerging Research in Information Assurance, Security and Privacy Services, S. Upadhyay and R.O. Rao (eds.), Emerald Group Publishing, pp. 421-452;2009.*

[18] *AvvariSirisha , G. Geetha Kumari: API Access Control in Cloud Using the Role Based Access Control Model", pp. 135- 137, IEEE , 2010.*

[19] *Amol Jadhao, Kunal Anand, Shashank Dhar, SagarMukharia: Cloud Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds, IJST, Vol 4, Sep – Oct 2016*

[20] *Ryan Shea,Jiangchuan Liu: Performance of Virtual Machines Under Networked Denial of Service Attacks: Experiments and Analysis, IEEE Systems Journal Volume: 7, Issue: 2, June2013.*

[21] *Justin LeJeune,Cara Tunstall,Kuo-pao Yang: An algorithmic approach to improving cloud security: The MIST and Malachi algorithms, IEEE Aerospace Conference,2016*

[22] *Jens Lindemann: Towards Abuse Detection and Prevention in IaaS Cloud Computing, IEEE International Conference on ARES, Aug2015.*

[23] *Jens Lindemann: Towards Abuse Detection and Prevention in IaaS Cloud Computing, University ofHamburg,Germany Publications, Aug 2015*

[24] *Qiao Yan,F. Richard Yu,Qingxiang Gong: Software- Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges, IEEE Communications Surveys & Tutorials (Volume: 18, Issue: 1, Firstquarter2016)*

[25] *R. Ashalatha, Jayashree Agarkhed: Multi tenancy issues in cloud computing for SaaS environment: Circuit, Power and Computing Technologies (ICCPCT), 2016 International IEEE Conference on 18 - 19 March2016*

[26] *Ingo Muller, Jun Han, Jean-Guy Schneider: Tackling the Loss of Control: Standards-Based Conjoint Management of Security Requirements for Cloud Services: Cloud Computing (CLOUD), 2011 IEEE International Conference on 4-9 July 2011*

[27] *Victor Ion Munteanu,Andrew Edmonds, Thomas M. Bohnert: Cloud Incident Management, Challenges, Research Directions, and Architectural Approach: Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on 8 - 11 Dec2014*