Information Security in Cloud Computing: A systematic Literature Review and Analysis

Dinesh Taneja, S S Tyagi
Manav Rachna International University, Faridabad India
dinesh.taneja@gmail.com

Abstract : Cloud computing is an evolutionary outgrowth of prior computing approaches which build upon existing and new technologies. Cloud computing is a model for on demand network access to a shared pool of resources such as servers, storage, applications and related services. Cloud computing can be provisioned and released with minimum interaction and preferably without intervention of cloud service provider. The rising awareness and implementations of cloud services and its underlying technologies cause the need for security requirements being up to date. These developments have created new security vulnerabilities, including security issues whose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and countermeasures. The security challenges in cloud computing are formidable, especially for public clouds whose infrastructure and computational resources are owned by an outside party that sells those services to the general public. Cloud security requirements have been addressed in publications earlier, but it is still difficult to estimate what kinds of requirements have been researched most, and which are still under-researched. This paper carries out a systematic literature review by identifying cloud computing security requirements from publications. Along with security issues, upside of information security in cloud computing has also been part of this work.

Keywords— Cloud Computing, Deployment Models, Literature Review, Security Issues, Service Models, Threats.

I. INTRODUCTION

The first draft of the cloud computing definition was created in November 2009. After years in the works and 15 drafts, the National Institute of Standards and Technology's (NIST) working definition of cloud computing, the 16th and final definition has been published as The NIST Definition of Cloud Computing (NIST Special Publication 800-145). According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing is majorly advocated as virtualization or multitenancy being the necessary cloud capability. But it is pertinent to mention that virtualization is not a must component of cloud computing. This particular approach is more popular due to the facts that it has helped to bring down the pricing and ease of deployment for pay per use model. Cloud computing grabbed the spotlight in past years and is becoming more popular because of less capital expenditure and management cost. General example of cloud services are Google Apps, Oracle Cloud, Microsoft Office 365 etc.

In rest of this research paper, cloud shall be referred for the term cloud computing. A cloud provides a cloud service user (CSU) the privilege of access to an application, platform or infrastructure “as a service” [1]. CSU is making use of the service which is provided by Cloud service provider (CSP).

National Institute of Standards and Technology (NIST), USA has defined three service models – Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). This is also majorly referred as SPI service model. However new term which is not defined by NIST but still becoming more popular in newsletters and conferences is XaaS which is a collective term said to stand for a number of things including "X as a service," "anything as a service" or "everything as a service." NIST has also defined four types of deployment models named as Private, community, Public and Hybrid models. The Information security in cloud is dependent on this various levels of controls in different service models and deployments. In various studies and surveys including that of International Data Corporation (IDC), security is the main challenge or blocker for adoptability of cloud computing technologies amongst various sections of the Industry. The rapid growth of cloud computing has brought many security challenges for users and cloud service providers. This is the main reason for going deep into this field and studies the probable threats in adoptability and prepare a literature review paper on major issues. The main focus of this research paper is on Public deployment of cloud because more security aspects are required to be dealt in this deployment model.

Problem Statement: Some research has been done in last few years on Cloud computing and security. The adoptability is increasing but not at the same pace in all segments of Industry such as Healthcare; this requires deeper insights into latest security threats in cloud and its associated solutions. The motive of this paper is to prepare a deeper and structured overview of the information security requirements in cloud and the proposed solution to these requirements. This paper also focuses on what is more published in empirical studies and what is still required to be researched further.

Research Question: Following Research questions are being addressed in this research paper.

RQ1: What are major information security issues and countermeasures which are commonly addressed by most of the publications?

RQ2: Are there any upside(s) of Information Security in cloud computing.

RQ3: Which Cloud Security issue is most under researched?

II. METHOD OF RESEARCH

A systematic literature study has been carried out to answer above mentioned research questions. Since research on cloud computing was more popular only in the last few years, therefore no limit on publication year was considered. We have considered certain constraints: studies included in the selected sources must be written in English and these sources must be web-available. Science Direct, ACM digital library, IEEE digital library, Scholar Google were considered as resources. An initial search on cloud computing and security issues was carried out and in total 97 papers was collected. In order to focus on the most relevant literatures, Security issues as mentioned in cloud Security guidelines documents from National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA) were considered. A primary evaluation was conducted based on reading the abstracts of all selected articles. The inclusion and exclusion criteria of this study were based on the research question as mentioned above. Some of the references as mentioned in the literature found from above mentioned sources were also taken into consideration. Additional related work exists, as several researchers have studied the field of cloud computing and its issues and challenges earlier, this paper concentrates on topics / issues which are now most researched and which are lacking in efforts of investigation for the mentioned purposes.

III. DISCUSSION ON INFORMATION SECURITY IN CLOUD COMPUTING.

The selected literature will now be evaluated on the common issues as enlisted by NIST and CSA guidelines. This evaluation of literature will also help us to identify the areas which are more researched as compared to other issues and which need further research. This will help us in determining recommendations on future work and research.

A. Data Handling

It is pertinent to mention that prospective cloud service adopters would have security concerns around storing and processing sensitive data [8]. Data is exposed at following states.

Data in Rest:- Data at rest refers to any data in computer storage and here it is being referred to data stored in CSP storage. In case of cloud since data is stored on providers storage and it is more in his control rather than client. Therefore it should be ensured that CSP follows standard Security policies and the data center of service provider is certified for at least the type of Industry of the client. If client is healthcare then data center should be HIPPA compliant and if the client is a bank then CSP data center should be PCI-DSS compliant and so on.[8]

Data in Motion:- Data in motion is referred to data as it is moved from a stored state to same or another form to a different location. Data in motion can also be referred to data in transition and not necessarily permanently stored. Even the username and password to access website is also ancillary data in motion.[8]

The Data handling issues are being discussed below.

Data Breach: To illustrate the potential magnitude of this threat, CSA pointed to a research paper how a virtual machine could use side-channel timing information to extract private cryptographic keys [4] [5] in use by other VMs on the same server. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but affect every other client’s data as well.

Data Loss & Leakage:- Data leakage happens when the data gets into the wrong hands while it is in rest, motion or under process. Data Loss Prevention (DLP) solutions detect and prevent unauthorized attempts to copy or send sensitive data, both intentionally or/and unintentionally, without authorization, by people who are authorized to access the sensitive information [12]. DLP solutions detect and prevent unauthorized attempts to copy or send sensitive data, both intentionally or/and unintentionally, without authorization, by people who are authorized to access the sensitive information

Data Scavenging:- Data Scavenging is the removal of sensitive data from a storage device in various situations, such as when a storage device is removed from service or moved elsewhere to be stored. Data scavenging also applies to backup copy created for restoration of services in certain circumstances. Since data cannot be completely removed from media unless the device is destroyed, attackers may be able to recover this data from media being replaced for maintenance or other reasons.[11]

Data Backup: - Data backup is an important aspect in order to facilitate recovery in case of disaster, but in case of cloud computing, it may introduce security concerns [3]. Sometimes cloud service providers outsource backup to third-party service providers, which may raise other legal issues.

Data Lock in:- The data is stored by service provider in proprietary CSP format and it cannot be easily exported or modified for a new environment. [8] Cloud service user should avoid data lock in and thoroughly discuss this with CSP before adopting this technology.

Data Ownership:- The organization’s ownership rights over the data must be firmly established in the service contract [1]. Intellectual property, including original works created using the cloud infrastructure, may be stored. The cloud customer should ensure that the contract respects their rights to any intellectual property or original works as far as possible without compromising the quality of service offered [7]. Cloud service User should also check the status of its Meta Data. Meta data is simply data about data.

Data Location:- When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Among the concerns to be addressed are whether the laws in the jurisdiction where the data was collected permit the flow, whether those laws continue to apply to the data post transfer, and whether the laws at the destination present additional risks or benefits. Technical, physical and administrative safeguards, such as access controls, often apply. Law & Regulations:- FISMA requires federal agencies to adequately protect their information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction; this is mandatory if the data is being managed by the agency or its third party contractor. There are some industry specific standards such as Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).[1]

Countermeasure for Data Handling:- Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability for exposure of content under their control remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf. These issues mainly happen due to insufficient Due Diligence. It is recommended that CSU has sufficient resources who can perform extensive due diligence before jumping into the cloud. Plain text that is developed over time may include important valuable records about users. CSU may ask for confidentiality of its meta data and destruction of this information permanently after the contract is terminated.

B. Service Traffic Hijacking

If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return modified / false information, and redirect your clients to unwilling sites. Your account or services instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.[21]

Countermeasure:- Organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible. Cloud Security Alliance (CSA) has issued an Identity and Access Management Guidance which provides a list of recommended best practices to be governed.[12].

C. Insecure Interfaces and APIs

System administrators rely on interfaces and Application Program Interface (API) for cloud provisioning, management, orchestration, and monitoring. Many a times, Organizations and third parties known to build on these interfaces, injecting add-on services to facilitate ease of system administration. Weak interfaces and APIs can expose an organization to such security issues pertaining to confidentiality, integrity, availability, and accountability.[6]

Countermeasure: - Organizations specially the providers and orchestration layer developers in the field of Cloud are required to understand the security implications associated with the usage, management, orchestration, and monitoring of cloud services and take necessary steps while developing such interface and APIs[6]

D. Denial of Service Attack

DoS has been a major threat for years, but it becomes more potential threats for CSP and CSU both. It is possible that a malicious user will take all the possible resources which has been hired by client on cloud and the system cannot satisfy any request from other legitimate users due to resources being unavailable. DoS [20] outages can cost service providers, customers and prove pricey to customers who are billed based on compute cycles, bandwidth and disk space consumed.

In today’s high bandwidth era and stronger security features implemented by CSP, an attacker may not succeed in knocking out a service entirely, but he may still cause it to consume so much processing time and unwanted bandwidth usage. Since CSUs are charged based on pay per use model for resources such as compute cycle, storage and bandwidth etc. In such cases it becomes too expensive for CSU to run and you'll be forced to take it down yourself.

Countermeasure:- Before selecting CSP, user must ask the questions for network architecture as available with provider. Some Internet Service providers provide internet bandwidth which is DDOS[24] protected; and CSP has deployed adequate security measures at gateway level which protects unwanted internet bandwidth usage and protects DOS attacks. This may help reducing unwanted usage charges and breakdowns.

E. Malicious Insider Attacks.

Malicious insiders can be a current or former employee, a contractor, or an outsourced third party who gains access to a network, system, or data for malicious purposes. These attacks are quite prominent for all three service models of Cloud Computing i.e. IaaS, PaaS, SaaS. Even if encryption is implemented and if the keys are not kept with the CSU and are only available at data-usage time, the system is still vulnerable to malicious insider attacks.

Countermeasure: Fog computing [13] which is suggested to include user behavior profiling and Decoy Information such as honey pots may be implemented to avoid malicious insider attacks.

F. Cloud Abuse

A legitimate hacker may use cloud servers hosted on same CSP or third party CSP to launch a DDoS attack, propagate malware, botnet etc.[10] Botnets have been used for sending spam, harvesting login credentials, and launching injection attacks against Websites. Botnets can also be used to launch a denial of service attack against the infrastructure of a cloud provider. Hacker may hire cloud services to launch phishing attacks, malware etc. This leads to another challenge for CSP to define what constitutes abuse and to determine the best processes for identify it.[22]

Countermeasure: A few solutions has been suggested by researchers such as intrusion prevention system, flitering of Network Traffic, Logging along with some non technical measures such as acceptable use policies, account verification etc.[23]

G. Multi Tenancy

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

Countermeasure:- The Infrastructure at CSP end should be designed and deployed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS).

H. System Complexity

A public cloud computing architecture is a bit complex as compared to in house deployment of the same service. A public cloud architecture like any in house solution may include application deployment, compute infrastructure, storage, supporting middleware, virtualization, third party VMs etc but it may additionally include other management backplanes such as for self-service resource allocation, quota management, metering, data replication and recovery management etc. Public cloud service itself may be a nested architecture provided by other third party cloud service providers. Therefore the security depends on more complex architecture.

Countermeasure: Subscriber of this service should take due diligence of the cloud architecture depending upon his requirement and keep all the aspects in its risk assessment plan.[7]

I. Loss of Control

Migrating to a public cloud requires a transfer of control to the cloud provider; your data and other system components that were previously under the client's direct control. This loss of control [26] will affect subscriber's ability to maintain situational awareness, find alternatives, prioritization of tasks best suited to the incident in favor of client's organization. Loss of control differs in three service models (Saas, Paas, Iaas).

Countermeasure: Due diligence is must to understand the architecture of the provider solution and risk assessment should be planned accordingly.

J. Virtualization Issues

We have discussed so far about multi tenancy, resource pooling etc; to achieve this, Virtualization of compute resources is one of the main building block of Cloud Architecture. Virtualization allows users to create, copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications. In Virtualization a second logical layer is added to create Virtual machines. Security becomes more complex due to additional layer and complex interconnectivity [14].

Shared Resources:- Virtual machines hosted on same physical server share CPU, memory, I/O, network etc. Sharing resources between virtual machines may cause security issue amongst different virtual machines. For example, a malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor. VM escape, the program running in a virtual machine is able to completely bypass the virtual layer (hypervisor layer), and get access to the host machine.

Uncontrolled VM Images:- In virtualization, a VM image is a prepackaged software template containing the configurations files that are used to create new virtual machines. One can either create its own image from scratch, or one can use any image stored in the service provider's repository. An attacker with a valid account can create an image containing malicious code. If another customer uses this image to create VM, the new virtual machine will be infected with the hidden malware. So these images can be the fundamental for overall security of virtualization [15].

Exposed IP Address of VMs:- Network components may also be shared by different clients due to resource pooling. In virtualization, virtual networks are configured either by bridging or routing in virtual switch of hypervisor. This may lead to perform some attacks such as sniffing and spoofing virtual networks. VMs have IP addresses that may be visible to anyone within the cloud and hence the attacker may map the target virtual machine [17]

Countermeasure: The issues due to Virtualization may be solved by properly configuring the host/guest interaction. [14] Traditionally firewalls are configured at gateways but for better security countermeasures, the firewalls may be configured near to the virtualization hypervisor.

K. Compliance & Governance

As per NIST guidelines, “Compliance involves conformance with an established specification, standard, regulation, or law. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.” Many a times, organizations embrace the cloud without fully understanding the particular CSP cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. Like a CSP is having Disaster recovery site in another country and the “Law of Land” is referred in contractual agreements and the DR site country law may state that it can have access to the data stored in the data centers deployed in their country for some specific reasons. In this way the data confidentiality is at stake of the CSU.

As per NIST guidelines on Security and Privacy in Public Cloud Computing; “Governance implies control and oversight over policies, procedures, and standards for application development, as well as the design, implementation, testing, and monitoring of deployed services”. A study involving more than nine hundred information technology professionals in Europe and the United States indicates a strong concern by participants that cloud computing services may have been deployed without their knowledge in parts of their respective organization. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing.

Countermeasure:- To manage governance, the organizations / CSU should make a risk management program which can deal with continuously evolving and shifting risk landscape. Any deployment over CSP should be evaluated by Risk management program. The CSU should have audit mechanisms in place to determine how data is stored, protected and used and also consider rest of the probable threats as majorly discussed in this research paper.

L. Service Level Agreements

An SLA represents the understanding between the cloud subscriber and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation available to the cloud subscriber.[1]

Countermeasure:- Exit Clause must be mentioned with proper data transfer, data sanitization, service transition. In case the client wishes to migrate service to any third party service provider, the present Cloud service provider should provide disposition support including data migration, knowledge transfer and integration respectively.

M. Incident Response

Incident responds means dealing with Information Security incidents in an organized manner. Incident management [27] shall include logging of incident, incident verification, root cause analysis of attacks, containment (restrict effected area of incident), data collection and preservation, problem remediation, and service restoration. Response to an incident should be handled in a way that limits damage and reduces recovery time and costs else it may lead to problems for other customers of same CSP.

Countermeasure: The Contract agreement between CSP and CSU must provision procedures incident response and management. The CSP should transparently share the information with its clients during and after the incident.

IV. ANALYSIS OF INFORMATION SECURITY ISSUES IN CLOUD COMPUTING:

The issues as mentioned above can be broadly classified into three categories based on its nature i.e. Technical, Legal or procedural. Some of the issues may be part of one or more classification category as mentioned in Table 1 below.

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

Table1: Classification of Information Security Issues in cloud computing.

V. UPSIDE OF INFORMATION SECURITY IN CLOUD COMPUTING:-

Almost all the literature has mentioned Information Security in cloud computing as either threat, issue, vulnerability, risks. On the other hand, small and mid-size organizations may derive security benefits from transitioning to a public cloud computing environment. Some of those benefits are being discussed here.[1]

a) Staff Specialization:- For smaller organizations, with increase in scale of computing, the IT administrators has to concentrate on other duties and organization may benefit from more experienced staff available with Cloud service provider.

b) Platform Strength:- Usually Homogeneity and uniformity is maintained in Service Provider’s Infrastructure, therefore Patch management and software hardening activities are more managed as compared to a small organization’s own data center. A small organization chooses Cloud service provider which is already complied with international Standard such HIPPA, PCI-DSS etc.

c) Business Continuity Plan:- The backup and recovery policies and procedures of a cloud service may be superior to that of a small organization. CSP might have maintained Disaster Recovery site at a geographically distant location which is otherwise very costly for a small organization.

d) Cloud Oriented Security:- Security as a Service is also available and becoming popular with due course of time. It is difficult for smaller organizations to invest and implement best security practices at its own due to cost and lack of expertise. As an example, an organization can transfer email via cloud centered security system by just redirecting their MX records. Security as a service is cost effective and useful for small organizations and it is becoming quite popular in the areas of Identity Services and Access management, Data Loss Prevention, Web Security, Email Security, Intrusion Detection and Prevention System, Network Security etc.

VI. CONCLUSION:-

Cloud computing is becoming popular because of its cost and other good number of reasons for its users. At the same time its adoptability may be faster if security aspects are addressed well. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture which is composed of a combination of different complex technologies. New Security techniques are required to be developed so as to meet cloud architecture. An analysis of security has been done on the basis of three popular service models (SPI) of cloud computing.

The upside of security in cloud computing has also been presented; at the same time it is recommended that due Diligence is must before adopting Cloud computing. It is recommended that cloud service provider must educate and share the risk mitigation document with client.

It is recommended that Information security in cloud computing should not be seen as technical issues only but one has to carefully plan the security and privacy aspects considering Legal, Procedural and Technical issues.

This paper reports on a systematic review carried out to answer three research questions which were raised in section 1.2. The key findings to question RQ1 is given in Section 3 of this paper. The key findings of the upside of Information security in cloud computing is also mentioned in section 4 of this paper. About RQ3, as per our assessment, cloud abuse is the security issue which is the most under researched area followed by one of data handling issue which is Disposition Support at the time of migration of service from one provider to another.

REFERENCES:

i. *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.*

ii. *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*

iii. *Subashini, S. and Kavitha, V: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34; 1 2011.*

iv. *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.*

v. *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; May 2011.*

vi. *ENISA: Cloud Computing: benefits, risks and recommendations for information Security; 2009.*

vii. *Vic (J.R.) Winkler: Securing the Cloud Cloud Computer Security Techniques and Tactics; Jun 2011*

viii. *Ronald L. Krutz Russell Dean Vines: Cloud Security A Comprehensive Guide to Secure Cloud Computing; July 2010*

ix. *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; June 2013.*

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

xi. *Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V3.0; 2009*

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

xiii. *Reuben JS: A survey on virtual machine Security. Seminar on Network Security; Technical report, Helsinki University of Technology; October 2007*

xiv. *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.*

xv. *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,*

xvi. *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.*

xvii. *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.*

xviii. *Avvari Sirisha , G. Geetha Kumari: API Access Control in Cloud Using the Role Based Access Control Model", pp. 135-137, IEEE , 2010.*

xix. *Amol Jadhao, Kunal Anand, Shashank Dhar, Sagar Mukharia: Cloud Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds, IJST, Vol 4, Sep – Oct 2016*

xx. *Ryan Shea, Jiangchuan Liu: Performance of Virtual Machines Under Networked Denial of Service Attacks: Experiments and Analysis, IEEE Systems Journal Volume: 7, Issue: 2, June 2013.*

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

xxii. *Jens Lindemann: Towards Abuse Detection and Prevention in IaaS Cloud Computing, IEEE International Conference on ARES, Aug 2015.*

xxiii. *Jens Lindemann: Towards Abuse Detection and Prevention in IaaS Cloud Computing, University of Hamburg, Germany Publications, Aug 2015*

xxiv. *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, Firstquarter 2016)*

xxv. *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 March 2016*

xxvi. *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*

xxvii. *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 Dec 2014*