International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-6, Issue No.-6, November, 2018

# A Survey of Security Violations and Prevention in Cloud Platform

Rethishkumar S.
Research Scholar, School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala.
rethishsnair3@gmail.com

Dr. R. Vijayakumar
Professor, School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala.
vijayakumar@mgu.ac.in

**Abstract**:-- The term "cloud computing" is everywhere. In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. Cloud computing is shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. The main thing that grabs the organizations to adapt the cloud computing technology is cost reduction through optimized and efficient computing, but there are various vulnerabilities and threads in cloud computing that affect its security. Providing security in such a system is a major concern as it uses public network to transmit data to a remote server. Therefore the biggest problem of cloud computing system is its security. In this paper we discussed different type of security issue related to cloud computing and some possible solution for them.

**Keywords**:-- Cloud Framework, Types, Service Providers & Models, Threats & Remedies.

## I. INTRODUCTION

Cloud computing is basically a collection of different services provided by different companies. It mainly depends on resource sharing using internet enabled devices that allow the function of application software. The Cloud can serve a wide range of functions over the Internet, such as storage from virtual servers, virtual applications, authorization of desktop applications etc. By implementing resource sharing, cloud computing is able to achieve reliability and economies of scale.

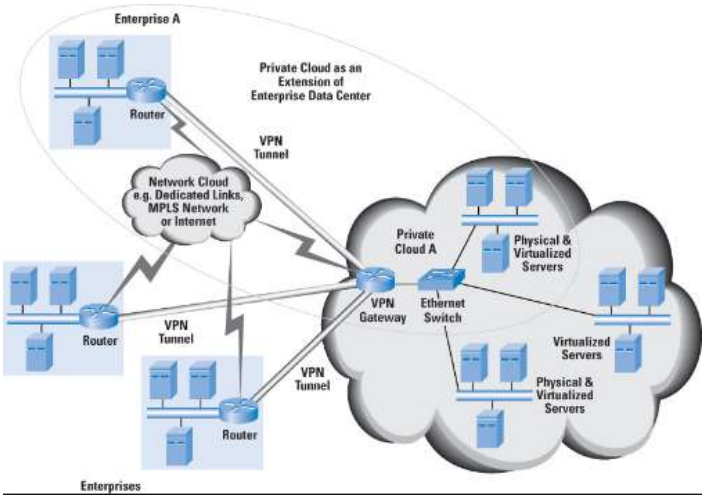


Image 1 – Infrastructure of a Cloud Network

**Characteristics:** essential characteristics of cloud computing:

i. On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

ii. Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations).

iii. Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.

iv. Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

v. Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for the provider and consumer.

**Types:** four Types of Cloud Computing Models are Based on a deployment model, we can classify cloud as:

- public
- private
- hybrid
- community cloud

*Public Cloud*: When we talk about public cloud, we mean that the whole computing infrastructure is located on the premises of a cloud computing company that offers the cloud service. The location remains, thus, separate from the customer and he has no physical control over the infrastructure. As public clouds use shared resources, they do excel mostly in performance, but are also most vulnerable to various attacks.

*Private Cloud*: Private Cloud provides the same benefits of Public Cloud, but uses dedicated, private hardware. Private cloud means using a cloud infrastructure (network) solely by one customer/organization. It is not shared with others, yet it is remotely located. The companies have an option of choosing an on-premise private cloud as well, which is more expensive, but they do have a physical control over the infrastructure.

*Hybrid Cloud*: Hybrid cloud, of course, means, using both private and public clouds, depending on their purpose. For example, public cloud can be used to interact with customers, while keeping their data secured through a private cloud. Most people associate traditional public cloud service with elastic scalability and the ability to handle constant shifts in demand. However, performance issues can arise for certain data-intensive or high-availability workloads.

*Community cloud* implies an infrastructure that is shared between organizations, usually with the shared data and data management concerns. For example, a community cloud can belong to a government of a single country. Community clouds can be located both on and off the premises. As explained before, the most common cloud service is that one offering data storage disks and virtual servers, i.e. infrastructure. Examples of Infrastructure-as-a-Service (IaaS) companies are Amazon, Rackspace, Flexiscale.

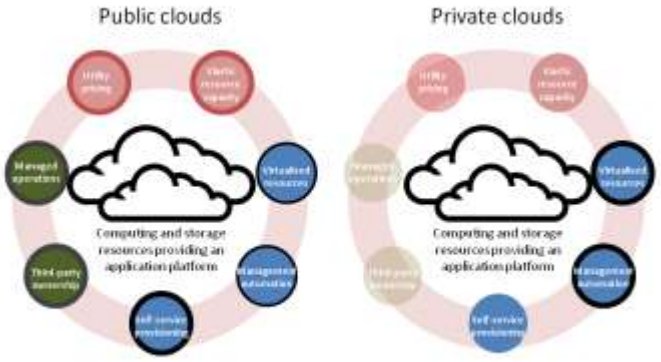


Image 2 – Private vs Public Cloud

**Service models**

Based on a service the cloud model is offering, we are speaking of either:

- IaaS (Infrastructure-as-a-Service)
- PaaS (Platform-as-a-Service)
- SaaS (Software-as-a-Service)
- or, Storage, Database, Information, Process, Application, Integration, Security, Management, Testing-as-a-service.

If the cloud offers a development platform, and this includes operating system, programming language execution environment, database, and web server, the model is known as Platform-as-a-Service (PaaS), examples of which are Google App Engine, Microsoft Azure, Salesforce. Operating system can be frequently upgraded and developed with PaaS, services can be obtained from diverse sources, and programming can be worked in teams (geographically distributed).

Software-as-a-Service (SaaS), finally, means that users can access various software applications on a pay-per-use basis. As opposed to buying licensed programs, often very expensive. Examples of such services include widely used GMail, or Google Docs.

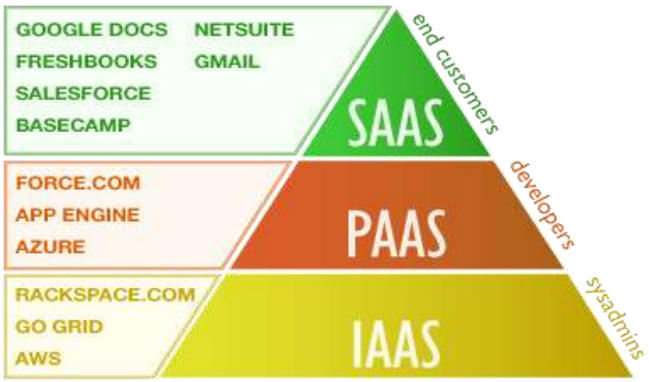


Image 3 – Cloud Services Types and Examples

The longer list will include Storage as a service (STaaS), Security as a service (SECaaS), Data as a service (DaaS), Test environment as a service (TEaaS), Desktop as a service(DaaS), API as a service (APIaaS).

**Pros and Cons**

Neither Cloud Computing is an exception and experience both prons and cons. Some of them are stated and described in more details in this chapter.

**Pros**

- **Lower costs** - the principle of sharing resources (HW, SW, infrastructure...) gives to customer also the benefit of sharing its costs. Customer do not has to buy expensive hardware, such as powerful workstations, large server solution and software applications. Customer needs only internet connection and basic PC with not high requirements. Simple laptop, netbook or

mobile phone is enough. Customer also pays only for what the real usege. These could be services, hardware resources or infrastructure or its combination.

- **Less IT employees** - there is also no necessary by customer to employ IT department in such wide range. There is only need to provide secure connection and PC with web browser. For all other, the technical support such as back-ups, recovery, virus protection, updates, software and hardware stability and functionality, helpdesk and support is maintained by the provider of a service.
- **No special knowledge** - client (customer) also does not need to have a high knowledge about hardware and complex software applications at all. Client just uses a service through web browser. Hardware resources can be shared between all clients and managed by usage or their requirements.
- **Easy to upgrade** - massive increase of performance (such as speed or storage size) is provided immediately after simple order and applied by "a few clicks". Data centre can provide higher performance than common desktop PC or, on the other hand, can be very efficient and deliver just what customer needs at the moment (low performance) and thus again it saves resources and money. This approach saves also time, costs for new hardware, transport, is power (energy) efficient and as a result saves the environment, which is very discussed issue these days.
- **Instant access anywhere** - one of the most important benefit is availability of a service anywhere. What is needed for accessing the service is computer connected to the internet. There is no dependence on platform (PC, MAC, mobile phone, car etc.).
- **Security** - is a very discussed issue in the Cloud Computing service providing and could be put in both pros and cons as you see in a while. Service is protected by usage an authorization. Users identify themselves by using an ID (Username) and Password (or also more sophisticated method such as chip, fingerprint, face detection etc. can be used). Communication between client and provider servers is secured. Data centre is protected by firewalls and kept in secured buildings. There generally there is a very low risk of danger caused by attack of third parties.
- **Requirements** - technology, which customer needs are very simple. Important is only terminal as a laptop, desktop, mobile phone, netbook etc. with web- browser, internet connection and usually also created account on a service at providers place.

**Cons**

- **Legal differences** – as already aforementioned, we can describe one particular example. US companies are obliged to follow the PATRIOT Act (2001) which states that companies can be watched and have to provide information and data about clients, if they are asked for in the correspondence of anti-terrorist policy.
- **Dependence on provider** – if company starts using the Cloud Computing service and replaces its previous information system or changes IT structure, it becomes dependant on its service provider. Risks connected with such a dependency may include sudden change of prices or conditions of a contract. Provider could be hit by bankruptcy and end its business activities. Functions and applications might be changed without will of a customer and if a provider suffers from technical problems, all the customers are out of service which means without their data.
- **Reputation** – Cloud Computing is very new type of service. Not many companies has an experience with such a kind of services and application outsourcing. Many users are still worried about data security tranmitted over the internet.
- **Migration costs** – in some cases there can be higher start- up costs. Company may have to invest into users training, any amendments which allows the communication of service provider and current company software and in some cases, switching to Cloud Computing could lead to a change of business processes.
- **Less functions** – solutions, which are targeted to the wide range of companies that can't provide specific functions and therefore are not flexible.
- **Dependence on internet connection** - all the Cloud Computing applications can be used on- line only thus any connection failure could be fatal.

## II. PROBLEM DEFINITION

**Virtual Machines:** A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine is comprised of a set of specification and configuration files and is backed by the physical resources of a host. Every virtual machine has virtual devices that provide the same functionality as physical hardware and have additional benefits in terms of portability, manageability, and security. A virtual machine consists of several types of files that you store on a supported storage device.

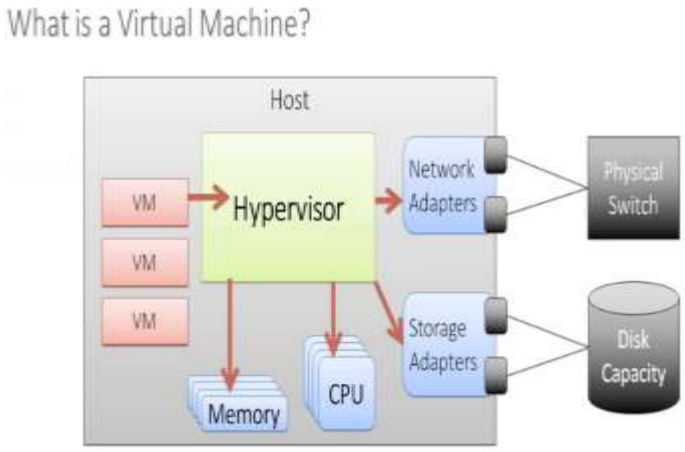


Image 4 – Working of Virtual Machines in Cloud

Virtual machines are becoming more common with the evolution of virtualization technology. Virtual machines are often created to perform certain tasks that are different than tasks performed in a host environment. Virtual machines are

implemented by software emulation methods or hardware virtualization techniques. Depending on their use and level of correspondence to any physical computer, virtual machines can be divided into two categories:

1. System Virtual Machines: A system platform that supports the sharing of the host computer's physical resources between multiple virtual machines, each running with its own copy of the operating system. The virtualization technique is provided by a software layer known as a hypervisor, which can run either on bare hardware or on top of an operating system.
2. Process Virtual Machine: Designed to provide a platform-independent programming environment that masks the information of the underlying hardware or operating system and allows program execution to take place in the same way on any given platform.

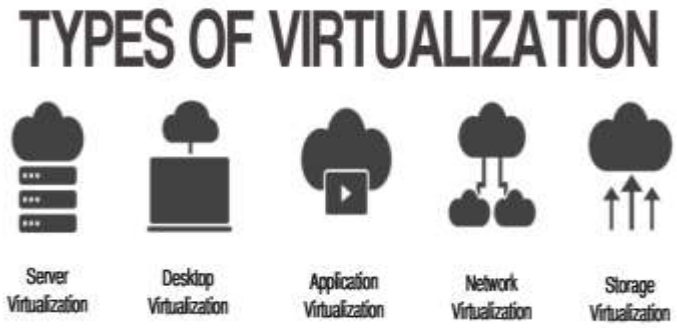


Image 5 – Types of Virtualisation in Cloud

Some of the advantages of a virtual machine include:

- Allows multiple operating system environments on a single physical computer without any intervention
- Virtual machines are widely available and are easy to manage and maintain.
- Offers application provisioning and disaster recovery options

Some of the drawbacks of virtual machines include:

- They are not as efficient as a physical computer because the hardware resources are distributed in an indirect way.
- Multiple VMs running on a single physical machine can deliver unstable performance.

**Various Attacks in Cloud Platform**

Key Cloud Computing Vulnerabilities:

- *Data threats:* Cloud users store various types of data in cloud environments, and a lot of that data contains sensitive information about users or business activities. However, this data is susceptible to loss, breach, or damage as the result of human actions, application vulnerabilities, and unforeseen emergencies. It's obvious that a cloud service provider can't prevent all data threats, but cloud developers should apply modern encryption algorithms to ensure the integrity of data in transit from the user to the cloud.
- *Cloud API vulnerabilities:* Application programming interfaces (APIs) allow users to interact with cloud-based services. However, vulnerabilities in APIs may significantly impact the security of cloud orchestration, management, provisioning, and monitoring. Cloud developers need to implement strong controls over APIs.
- *Malicious insiders:* Legitimate cloud users who act maliciously have many ways to arrange attacks or leak data in cloud environments. This threat can be minimized by cloud developers, however, by implementing identity and access management (IAM) technologies.
- *Shared technology vulnerabilities:* Cloud computing involves the use of shared technologies such as virtualization and cloud orchestration. Thus, by exploiting vulnerabilities in any part of these technologies, attackers can cause significant damage to many cloud users. Weaknesses in a hypervisor can allow hackers to gain control over virtual machines or even the host itself.
- *Provider lock-in:* Most modern cloud service providers make their clients dependent on their services with high switching costs. Many cloud users feel locked in when providers aren't able to provide all the services they need. Make sure that your solution has tools to help users easily migrate from other providers, such as the ability to import data in various formats.
- *Weak cryptography:* Though cloud providers use cryptographic algorithms to protect data in storage, they usually use limited sources of entropy (such as the time) to automatically generate random numbers for data encryption. For instance, Linux-based virtual machines generate random keys only from the exact millisecond. This may not be enough for strong data encryption, however, as attackers also use sophisticated decoding mechanisms to hack information. Thus, cloud developers should think about how to secure data before it moves to the cloud.
- *Vulnerable cloud services:* While cloud computing platforms are designed as distributed systems of cloud services, these services have little protection against each other. Thus, an attacker can exploit vulnerabilities in any one cloud service to gain unauthorized access to data of legitimate users. For instance, the OpenStack cloud platform had more than 150 known weaknesses in its cloud services in 2016. Creating a strong architecture can isolate a user's operations in the cloud.

**10 Most Common Types of Attacks on Cloud Computing**

There are many ways to attack cloud computing services, and hackers are constantly working on developing more sophisticated ones. However, becoming aware of at least the most common will help cloud developers design more secure solutions. Here's a list of the ten most common types of cyber attacks performed against cloud users.

*1. Cloud malware injection attacks:* Malware injection attacks are done to take control of a user's information in the cloud. For this purpose, hackers add an infected service

implementation module to a SaaS or PaaS solution or a virtual machine instance to an IaaS solution. If the cloud system is successfully deceived, it will redirect the cloud user's requests to the hacker's module or instance, initiating the execution of malicious code. Then the attacker can begin their malicious activity such as manipulating or stealing data or eavesdropping. The most common forms of malware injection attacks are cross-site scripting attacks and SQL injection attacks.

2. *Abuse of cloud services:* Hackers can use cheap cloud services to arrange DoS and brute force attacks on target users, companies, and even other cloud providers. For instance, security experts Bryan and Anderson arranged a DoS attack by exploiting capacities of Amazon's EC2 cloud infrastructure in 2010. As a result, they managed to make their client unavailable on the internet by spending only $6 to rent virtual services. An example of a brute force attack was demonstrated by Thomas Roth at the 2011 Black Hat Technical Security Conference.

3. *Denial of service attacks:* DoS attacks are designed to overload a system and make services unavailable to its users. These attacks are especially dangerous for cloud computing systems, as many users may suffer as the result of flooding even a single cloud server. In case of high workload, cloud systems begin to provide more computational power by involving more virtual machines and service instances. In the cloud environment, DDoS attacks may be even more dangerous if hackers use more zombie machines to attack a large number of systems.

4. *Side channel attacks:* A side channel attack is arranged by hackers when they place a malicious virtual machine on the same host as the target virtual machine. During a side channel attack, hackers target system implementations of cryptographic algorithms. However, this type of threat can be avoided with a secure system design.

5. *Wrapping attacks:* A wrapping attack is an example of a man-in-the-middle attack in the cloud environment. Cloud computing is vulnerable to wrapping attacks because cloud users typically connect to services via a web browser. An XML signature is used to protect users' credentials from unauthorized access, but this signature doesn't secure the positions in the document.

6. *Man-in-the-cloud attacks:* During this type of attack, hackers intercept and reconfigure cloud services by exploiting vulnerabilities in the synchronization token system so that during the next synchronization with the cloud, the synchronization token will be replaced with a new one that provides access to the attackers. Users may never know that their accounts have been hacked, as an attacker can put back the original synchronization tokens at any time. Moreover, there's a risk that compromised accounts will never be recovered.

7. *Insider attacks:* An insider attack is initiated by a legitimate user who is purposefully violating the security policy. In a cloud environment, an attacker can be a cloud provider administrator or an employee of a client company with extensive privileges. To prevent malicious activity of this type, cloud developers should design secure architectures with different levels of access to cloud services.

8. *Account or service hijacking:* Account or service hijacking is achieved after gaining access to a user's credentials. There are various techniques for achieving this, from fishing to spyware to cookie poisoning. Once a cloud account has been hacked, attackers can obtain a user's personal information or corporate data and compromise cloud computing services. For instance, an employee of Salesforce, a SaaS vendor, became the victim of a phishing scam which led to the exposure of all of the company's client accounts in 2007.

9. *Advanced persistent threats (APTs):* APTs are attacks that let hackers continuously steal sensitive data stored in the cloud or exploit cloud services without being noticed by legitimate users. The duration of these attacks allows hackers to adapt to security measures against them. Once unauthorized access is established, hackers can move through data center networks and use network traffic for their malicious activity.

10. *New attacks: Spectre and Meltdown:* These two types of cyber attacks appeared earlier this year and have already become a new threat to cloud computing. With the help of malicious JavaScript code, adversaries can read encrypted data from memory by exploiting a design weakness in most modern processors. Both Spectre and Meltdown break the isolation between applications and the operating system, letting attackers read information from the kernel.

## III. RESULT & DISCUSSION

**7 Tips on How to Ensure the Security of Cloud-Based Solutions:** the dynamic nature of cloud services breaks the traditional security model used for on-site software. It's obvious that a cloud service provider is unable to ensure total security in the cloud. Part of the responsibility also lies with cloud users. While the best way to protect user data in the cloud is by providing a layered security approach, cloud service providers should implement industry best practices to ensure the utmost level of cloud security on their side. Here are seven tips on how cloud developers can ensure the security of their cloud-based solutions.

1. *Enhance security policies:* When providing cloud services, software vendors should limit the scope of their responsibility for protecting user data and operations in the cloud in their security policies. Inform your clients about what you do to ensure cloud security as well as what security measures they need to take on their side.

2. *Use strong authentication:* Stealing passwords is the most common way to access users' data and services in the cloud. Thus, cloud developers should implement strong authentication and identity management. Establish multi-factor authentication. There are various tools that require both static passwords and dynamic passwords. The latter confirms a user's credentials by providing a one-time password on a mobile phone or using biometric schemes or hardware tokens.

3. *Implement access management:* To increase the security of services, cloud developers should let cloud users assign role-based permissions to different administrators so that users only have the capabilities assigned to them. Moreover, cloud orchestration should enable privileged

users to establish the scope of other users' permissions according to their duties within the company.

4. *Protect data:* Data in the cloud environment needs to be encrypted at all stages of its transfer and storage:

- at the source (on the user's side)
- in transit (during its transfer from the user to the cloud server)
- at rest (when stored in the cloud database)

Data needs to be encrypted even before it goes to the cloud. Modern data encryption and tokenization technologies are an effective defense against account hijacking. Moreover, it's important to prove end-to-end encryption for protecting data in transit against man-in-the-middle attacks.

5. *Detect intrusions:* Provide your cloud-based solution with a fully managed intrusion detection system that can detect and inform about the malicious use of cloud services by intruders. Use an intrusion detection system that provides network monitoring and notifies about the abnormal behavior of insiders.

6. *Secure APIs and access:* Cloud developers should be sure that clients can access the application only through secure APIs. This might require limiting the range of IP addresses or providing access only through corporate networks or VPNs. However, this approach can be difficult to implement for public-facing applications. Thus, you can implement security protection via an API using special scripts, templates, and recipes. You can even go further and build security protection into your API.

7. *Protect cloud services:* Limiting access to cloud services is necessary to prevent attackers from gaining unauthorized access to a user's operations and data through weaknesses in cloud services. When designing cloud service architecture, minimize event handler permissions to only those necessary for executing specific operations. Moreover, you can restrict security decisions to only those cloud services that are trusted by users to manage their data security.

## IV. CONCLUSION

Successful cloud attacks on service providers are rare, but their impact can be enormous, both to a provider and to its customers. The risk of these cloud attacks is manageable, though it does require a broad approach that includes having the right security controls in place, monitoring their output in real-time, capacity planning and adequate change control policies. Cloud security issues are active area of research and experimentation. Lots of research is going on to address the issues like cloud security, data protection, virtualization and isolation of resources. In this paper we discuss Denial of Service (DoS) attacks, Cloud Malware Injection Attack, Side Channel Attacks, Authentication Attacks and Man-In-The-Middle Cryptographic Attacks of cloud computing and also provide some possible solutions. The concepts we have discussed here will help to build a strong architecture for security in the field of cloud computation.

## REFERENCES

[1]. H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource allocation for security services in mobile cloud computing," in Proc. IEEE INFOCOM'11,

[2]. Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

[3]. Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu, "SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environment," Sixth International Conference on Natural Computation, ICNC 2010,

[4]. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," ICPPW '10 Proceedings of the 2010 39th International Conference.

[5]. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[7].Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, "Automated Control in Cloud Computing: Opportunities and Challenges", Proc. of the 1st Workshop on Automated control for data centres and clouds, New York.

[8].Daniel Petri, "What You Need to Know About Securing Your Virtual Network," Jan. 8, 2009.

[9].John E. Dunn, "Spammers break Hotmail's CAPTCHA yet again", Tech-world, 16th Feb. 2009.

[10]. Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security," Annals of Faculty Engineering Hunedoara International Journal of Engineering.

[11]. Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing," Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

[12].Josh Karlin, Stephanie Forrest, Jennifer Rexford, "Autonomous Security for Autonomous Systems," Proc. of Complex Computer and Communication Networks; vol. 52, issue. 15, pp. 2908- 2923, Elsevier, NY, USA, 2008.

[13].Czaroma Roman, "Sony Data Breach Highlights Importance of Cloud Security," Cloud Times, May 9, 2011.

[14].Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media, Sep. 2009;

[15].Hamid R. Motahari-Nezhad, Claudio Bartolini, Sven Graupner, Sharad Singhal, Susan Spence, "IT Support Conversation Manager: A Conversation-Centered Approach and Tool for Managing Best Practice IT Processes".

[16]."Security Considerations White Paper for Cisco Smart Storage," Cisco Systems, 2010.

[17]. Pradnyesh Rane, "Securing SaaS Applications: A Cloud Security Perspective for Application Providers," Information Systems Security, 2010.

[18].Amitav Chakravartty, Serena Software, "Serena Service Manager Security in the Cloud".

## AUTHOR'S BIOGRAPHIES

Dr. R. Vijayakumar is currently working as Professor at School of Computer Sciences, Mahatma Gandhi University, Kottyam, Kerala. He was formerly acting as DCDC, Dean-Faculty of Engg & Tech., Chairman-BOS-CS and also Member of Syndicate of University. He had 30 years of teaching experience and his research area is Security and Privacy. He works as Co-Ordinator, AICTE, life member ISTE, CSI & ACEEE.

Mr. Rethishkumar S. was working as Lecturer in CSE Dept at University College of Engineering, Thodupuzha. His area of research is Cloud Security Strategies. He has published more than 5 papers in this field and attended more Conferences in the same scenario. Now he is doing research in School of Computer Sciences, Mahatma Gandhi University, Kottayam, Kerala. He is co-ordinating a lot of system related activities all over the University.