iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VI **Month of publication:** June 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue VI, June 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Security Issues and its Solution in Cloud Computing

Rahul Yadav [1], Uttara Athawale [2]
[1]PG Student, [2]Assistant Professor, BVIMIT, Navi Mumbai

Abstract*— Cloud computing is a rapidly increasing technology which includes splitting of computer resources. Cloud computing removes the necessity of having an entire infrastructure of hardware and software to meet user's needs and applications. The user gains access to software stored in the cloud network from a remote place by connecting to the cloud using the Internet. Despite having advantages which include multi-tenancy, resource pooling, storage capacity its various security faults including loss of sensitive data, data leakage and few others. As the technology of the cloud computing is increasing rapidly and implemented in different areas, legal/contractual, security and privacy issues still create significant challenges. Security is a major concern for corporate who have their businesses in cloud and sense a need for security. This paper identifies major challenges and highlights the techniques that are used to provide protection and privacy to reduce security risks and protect resources of various enterprises.

Keywords*— Cloud computing, cloud infrastructure, security challenges, security solutions, Cloud data.

I. INTRODUCTION

Cloud computing is a technology which allows convenient, easy and on-demand access to a shared pool of resources (eg. networks, servers, data storage, software, and services) that can be provided and delivered with minimal management or interaction with service provider. The major cloud providers include Amazon, Google, and Microsoft Azure. Some examples of applications which use Cloud Computing are Dropbox, Google Docs, Google Calendar, and Gmail etc. Cloud Computing utilizes large group of servers with specific connections to servers that provide distributed processing of data with other servers.

Cloud Computing works on distributed architecture that resources of centralized server on scalable platform so as to provide on demand computing services. The plan is to shift from desktop computing to a service-oriented platform via virtual server at data centers. Generally, cloud offers three types of services i.e. Platform-as-a-Service, Software-as-a- Service and Infrastructure-as-a-Service. The reasons for organizations to migrate to cloud computing include paying for the resources on consumption basis, make use of increasing computing power to execute millions of instructions per second, minimize the usage cost of computing resources and provide quality of service [1].The user does not require any knowledge to manage the infrastructure of clouds; it provides only abstraction.Cloud computing is seen as a business necessity, as it provides infrastructure without managing it.

Cloud computing is a technology that increases the capacity dynamically without requiring investing in infrastructure, training people, or buying new software. But as more and more data is being stored in the cloud, security concerns of the cloud environment begin to grow.

A. Cloud Computing Service Model

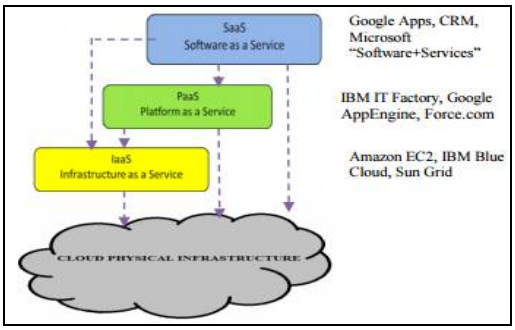


Fig. No. 1 Cloud service model

1) Infrastructure-as-a-Service (IaaS): Services include computation resources, data storage and network as an internet services.

Volume 4 Issue VI, June 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

This model is based on the virtualization technology. ex. Amazon EC2.

2) *Platform-as-a-service (PaaS):* Services include platforms, tools and other business services that allow customers to create and deploy their own applications, without installing any of these platforms by hosting on top of the cloud infrastructures .ex. Google Apps Engine and Microsoft Windows Azure.
3) *Software-as-a-service (SaaS):* Services include applications hosted on the cloud infrastructure such as services based on internet for users, applications. ex. SalesForce CRM.

II. NEED FOR SECURITY IN CLOUD COMPUTING

Security is the most important issue in cloud computing. According to the IDC's on the cloud services, security is the most important issue under cloud computing [4][5].

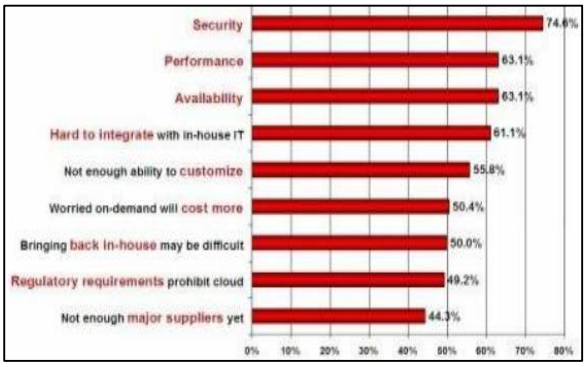


Fig. No. 2 Major issues in cloud computing

Cloud Computing security is a major problem to be addressed nowadays. If security mechanisms are not implemented for data operations and management then data is at risk [6]. Since cloud computing provides services to a group of users to access the stored information, there is a possibility of having data at risk. Strong security plan must implemented by identifying security issues and solutions to handle them.

Many businesses using cloud may not have the basic assets particularly from a security perspective. If there is a security breach occurs in cloud where data is stored, it would result in even more problems and damage. In the recent era, many companies are using cloud to store data about their organization, business and their customers. As a result, information classification becomes more vital. For ensuring data security, techniques such as encryption, logging, must be implemented. The challenge of preventing and detecting advanced threats and intruders must be solved. Not only security but also data privacy challenges exist in industries and corporate having data on cloud. With the increasing use of cloud in business, many organizations are dealing with privacy issues.

In a survey, 47% of those who currently use a cloud computing service reported they have encountered a data security issue or lapse with the cloud service their company. India had the highest rate of incident (67%), followed by Brazil (55%)[7].

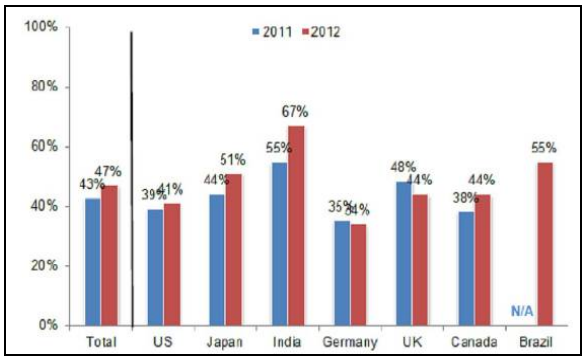


Fig. No. 3 Cloud security issues in various countries

III. SECURITY ISSUES AND CHALLENGES

The security issues in cloud computing infrastructure can be divided into network levels.

Network level: The issues that can be divided under network level include network protocols and network security, like distributed nodes, distributed data.
Authentication level: The issues that can be divided under user authentication level deals with encryption and decryption techniques, authentication methods like administrative rights, authentication of applications, and logging.
Data level: The issues that can be divided under data level deals with data integrity and privacy such as data protection.
Generic types: The issues that can be divided under general level are traditional security tools, and use different technologies.

A. Network security Challenges

1) *SQL injections:* Hackers inject a malicious code in order to gain unauthorized access to databases to manipulate the contents, retrieve confidential data or even take control of the web server.
2) *Cross-site scripting:* Hackers inject malicious scripts, such as JavaScript, VBScript and ActiveX into a web page to execute the scripts on victim's web browser. The attack could be used for illegal activities to access the victim's information.
3) *Man in the Middle attacks:* In this attack, an entity tries to intrude in an ongoing conversation between a cloud server and a client to insert false information and to access information about important data being transferred between them.
4) *Sniffer Attacks:* These types of attacks are created by applications which can collecr packets passing through a network and if the data is sent in these packets, it can be read if they are not encrypted. Packet sniffing is listening to the network for packets which are important.
5) *Denial of service attacks (DoS):* This attack is to make sure that targets computer resources become unavailable. The attacker aims to floods the victim with a large number of packets in a short duration of time to consume the whole bandwidth and resources of the target computer.

B. Data Security Challenges

1) *Data Integrity:* Sensitive data stored in cloud computing environment emerges as a major issue with regard to security in a cloud based system. Since anyone can access data from the cloud as the data may be public, private or sensitive. So concurrently, many cloud computing users and providers access and modify data. Thus there is a need of some mechanism to ensure data integrity in cloud computing.
2) *Data Loss and Leakage:* Data loss is a common problem in cloud computing. Data can be lost or damaged due to miss happening, natural disaster, and fire and there will be a loss of information. Data is always in danger of being lost or stolen by unauthorized access. Due to above situation, data may be inaccessible to users.
3) *Data Confidentiality:* Confidentiality means that only the authorized and intended users are given permission to access the data. Cloud Computing system offers applications and infrastructures which operate on public networks. Therefore, maintaining confidential data of user's secret in the cloud is a necessity.
4) *Losing control over data:* Exporting data means losing significant control over data. Large organization don't want to run a software delivered in the cloud that risk their data through interaction with some other software [8][9].
5) *Multi-tenancy:* One the main features of cloud computing is multi-tenancy. Since multi-tenancy allows storing data by multiple users on cloud servers, there is a possibility of intrusion by attacker. By injecting a client code data can be intruded.
6) *Privacy Issues:* The cloud service provider must take measures to ensure that customer information is isolated from other customer and user. As the servers are external, the cloud provider should identify who is maintaining and accessing the data and the server so as to protect the user information.

C. Cloud Security Challenges

1) Abuse of Cloud Computing Resources: A simple example of this is the use of malicious application to spread spam and malware. Intruders can access a public cloud and find a way to upload malware to computers in cloud and use the ability of the cloud environment to attack other systems.
2) Insecure Application Programming Interface: An API is used as an interface to interact with cloud services. They must have extremely secure authorization, access control, encryption and logging mechanism especially when third parties use them.
3)Malicious Insiders: The malicious insider is an important threat as many providers still don't disclose how they recruit people, how they grant them access to sensitive data or how they control them. Transparency is vital to create a secure cloud, along with compliance reporting and breach notification.

4) Authentication Process: Authentication is a critical function for every organization as data should not be accessible to unauthorized user. It ensures that only privileged user gets access to data and no intruder gets into cloud. Authorization describes which user has which privileges and what a user is allowed to do. It is the next step after authentication. Authentication can be determined based on user identity and/or by user role.

5) Access Control: Data stored on the cloud server can be accessed by people who are not privileged users such as employees of cloud service provider's company and there is no control over those people. If access control policy is not implemented properly, user's data will not remain secure.

6) Security related to Third-Party: A Trusted Third Party is an organization which allows secure interactions between two parties. The Third Party evaluates all critical communications between the parties. There is a need of transparency and control when a third party holds critical business data.

7) Logging: If logging is not present it is very difficult to identify if someone has breached the cloud or altering of data maliciously has occurred which needs to be reverted. In the absence of logging, internal users can do unauthorized data manipulations without getting noticed.

8) Virtual Machine Security: It brings new options for attackers because of the added layer. Security of Virtual machine becomes as important as physical machine security, and any vulnerability in one machine may affect the other. Virtual machine is vulnerable to all types of attacks for normal infrastructures.

IV. SOLUTIONS TO SECURITY CHALLENGES

A. Solution to Network Security

1) *SQL injection attacks:* Filtering techniques are used to sanitize the user data and check these attacks. SQL Injection attacks are prevented by using proxy based architecture which automatically extracts and detects users' inputs for suspected SQL control sequences has been proposed [20]. It is necessary to remove stored procedures that are not usually used. Also, allocate least possible privileges to users who have access to the database.

2) *Cross Site Scripting attacks:* Techniques like Web Application Vulnerability Detection, Content Based Data Leakage Prevention and Active Content Filtering, technique, technique are used to prevent this attacks [16]. These mechanisms use various methods to detect security flaws and fix them. An approach to minimize the dependency on web browsers is by spotting unchecked content over the network has been proposed in [17].

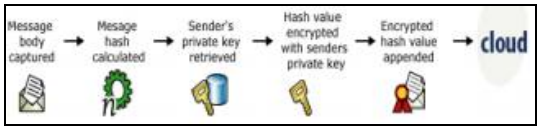
3) *Man in the Middle attacks:* It involves evaluating software as a service security [18]. Proper implementation of SSL configuration and data exchange tests between authorized parties can be useful to reduce the threat of this attack. Various tools implement strong encryption mechanism like: Dsniff, Ettercap, Wsniff and Airjack etc. have been developed to provide safeguard against them.

4) *Sniffer Attacks:* A sniffing detection mechanism using RTT (round trip time) and ARP (address resolution protocol) can be used to detect sniffing in a cloud running on a network [19]. If a hacker gets control over the hypervisor, he can manipulate the data passing through the hypervisor [20]. Stronger authentication and isolation between virtual machines can provide protection against such attacks.

5) *Denial of Service Attacks:* Intrusion Detection System is the most accepted technique to detect and take corrective actions to prevent it [21]. Behavior checking detects the attacks by identifying unusual behavior. Route based packet filtering and Secure Overlay Services are used to prevent this attack. Using strong firewall can also prevent this attack.

B. Solutions to Data Security

1) *Data Integrity Solution:* To solve this issue concept of public key cryptography using Digital Signature is used. A hash value is calculated and encrypted using senders private key and appended to the message and stored in cloud. When attacker changes data, the hash calculated by cloud by will not match hash of new message and changes are not accepted.



2) *Data Loss Solution:* Cloud Service provider needs to ensure that all sensitive enterprise data is regularly backed up to allow quick recovery in case of disasters. Also use of strong encryption mechanism to protect backup data is advised to prevent

leakage of information.

3) *Data confidentiality Solution***:** This can be achieved through cryptographic techniques, where a client can check the integrity of his data by storing a hash in local memory and authenticates by calculating the hash of the received data and comparing it to the value stored locally. The cloud provider should identify and who is controlling and accessing the data the server so as to protect the user information.
4) *Losing control over data Solution:* Control over data is achieved by allowing access to data through authentication of the request using HMAC-SHA1 signature using the user's private key [10][11][12]. Also encrypt the data before storing it in cloud. Therefore, the customer has complete control over access to their data. [13].
5) *Multi tenancy Solution:* There is a need to store data independently from other customer's data. Problems with data multi tenancy can be detected using the tests such as SQL injection, data validation. To ensure that customers don't cross over each other's territory, monitoring and strong isolation is required. Another effective measure is to monitor environment for unauthorized activity, and promote strong access control and authentication and for administrative access.
6) *Data Privacy Solution:* Cloud services encrypt the user's data using a strong encryption technique like RSA. Data masking is another technique that is intended to hide all identifiable characteristics from data. This technique is aimed at reducing the risk of exposing sensitive information. This method is used to preserve the privacy of records and involves substitution of actual data values with keys to an external table that holds the actual data values.

C. *Solutions to Cloud Security*

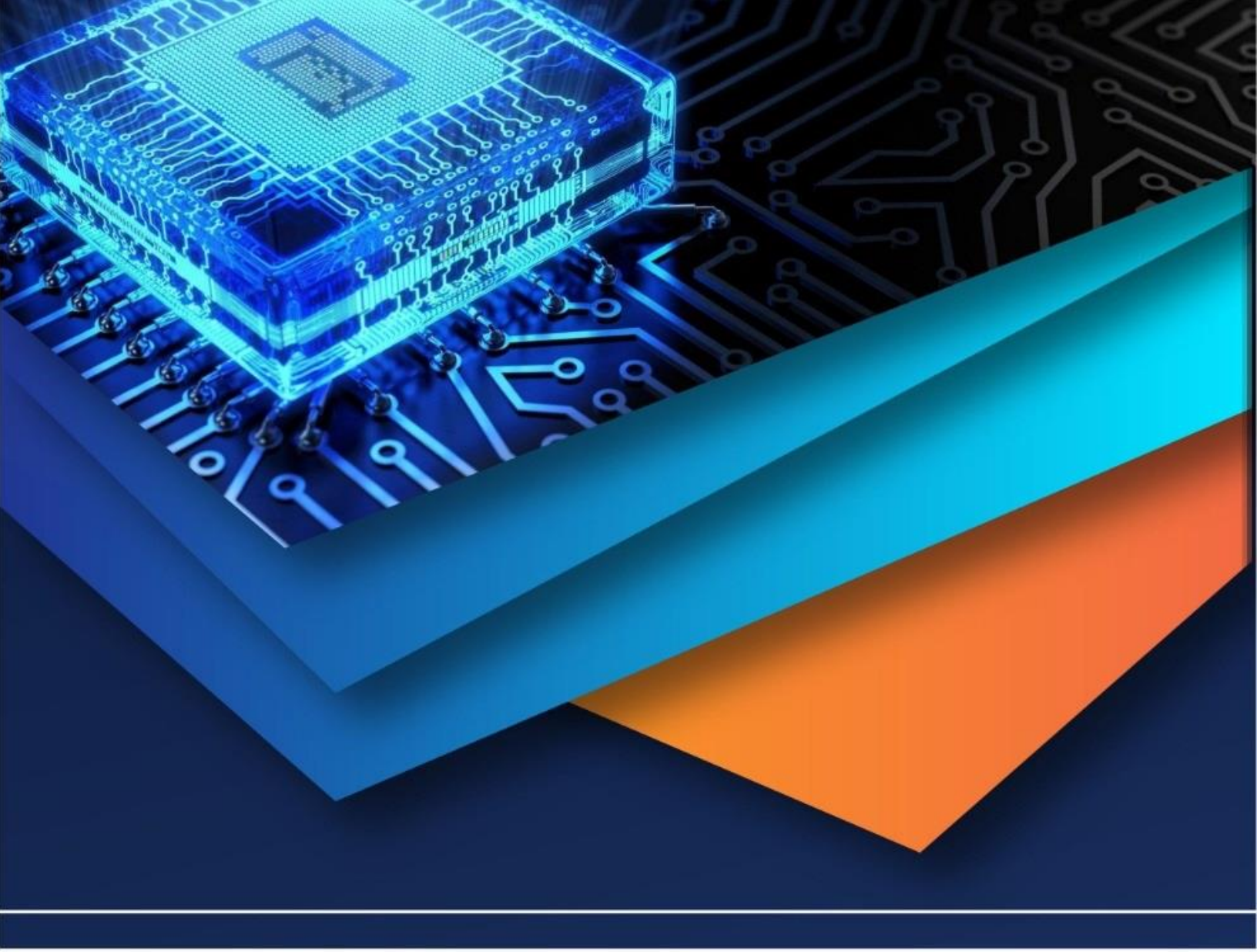
1) *Abuse and Use of Cloud Computing Solution:* It can be checked by implementing strict initial registration and validation processes. Another effective way is to enhance monitoring and coordination, and regular introspection of customer network traffic. Another useful step to take is to monitor public blacklists network blocks.
2) *Insecure Application Programming Interfaces Solution:* It can be checked by analyzing the security model of cloud provider interfaces. Another effective way is to ensure strong access controls and authentication are implemented with encrypted transmission and to understand the dependency chain associated with the API.
3) *Confronting Malicious Insiders Solution:* It can be checked by conducting a complete supplier assessment. Another effective way is to specify requirements as part of legal contracts, and transparency into overall information security and administrative policies. Implementing the access control matrix model reduces the access to the resources and function properly in their roles and responsibilities.
4) *Authentication Solution:* Authentication is achieved by various means, but all use a combination of authentication factors, something that an individual knows ex. a password, something they possess ex. a security token, or some quality that is intrinsic to them ex. a fingerprint. Stronger authentication requires two authentication factors such ex. a pin and a fingerprint. Another way to authenticate is by using Kerberos, using Key Distribution Centre and Public Key Infrastructure.
5) *Access control:* To apply access control, the cloud service provider must describe and ensure that only legitimate users can access the user or consumer's data. The different access controls are:
   Discretionary Access Control (DAC) - In DAC, access control is decided by the owner of the object who decides who can access and what privileges they will have.
   Role Based Access Control (RBAC) [14][15] - Access control is decided by the system. In RBAC access is assigned on the role of subject. A subject can use an object if their set of permissions allows it.
   Mandatory Access Control (MAC)-Access control is decided by the system and is implemented by labels, which are allocated to subject and object. A subject's label defines its degree of trust, and an object's label defines the degree of trust which is required to access it. If a subject wants to gain access to an object, the subject must be at least as high as the object.
6) *Third Party Solution:* Some of the security requirements of third party are low and high level confidentiality and privacy, server and client authentication, separation of data, and certificate based authorization. A Trusted Third Party should be an impartial company delivering business confidence by providing technical security features to electronic transactions.
7) *Logging Solution:* All activities performed by users in cloud should be recorded by logging. These logs must be checked frequently to find any unauthorized activity performed by any user.
8) *Virtual machine Solution:* To effectively protect virtual machines, they should be isolated from other network and deep checking at the network level should be implemented to prevent them from internal and external attacks. Internal attacks can be restricted by applying by intrusion prevention systems and external attacks can be protected by implementing secure technologies like IPSec or SSL VPN.

V. CONCLUSION

Cloud computing has gained a lot of interest worldwide because of its lower cost, reduced complexity for customers, and easier acquisition of services. With the benefits it also brings various security challenges. Many large financial company and businesses are still concerned about their data. In this paper, we identify the need for security in cloud computing. We also analyzed the security issues in clouds from three perspectives network security, data security and cloud security and discussed its solution. There is a necessity to make cloud more secure and robust to adapt to the requirements. Research is taking place in this area to find and standardize security in cloud environment. Cloud service providers should solve and implement these solutions on their cloud environment, to accomplish security and take advantage of cloud computing.

REFERENCES

[1] Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3
[2] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.
[3] Rohit Bhadauria et. al. paper on "A Survey on Security Issues in Cloud Computing". hib, HP, India, July 2011.
[4] Anthony T.Velte, Toby J.Velte and Robert Elsenpeter 2010. Cloud Computing- A Practical Approach. Publishing of Tata McGRAW Hil.
[5] Nils Gruschka and Meiko Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services". IEEE rd International Confrence on Cloud Computing,2010.
[6] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control incloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.
[7] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve, "Cloud computing security: Routing and DNS security threats
[8] John Viega, McAffee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.
[9] Marco Descher, Philip Masser, Thomas Feilhauer, A Min Tjoa, David Huemer, " Retaining Data Control to the Client Infrastructure Clouds", published on the IEEE, 2009 International Conference on Availability, Reliability and Security, pp. 9-15
[10] Amazon White Paper, http://aws.amazon.com/about-aws/whatsnew/2009/06/08/new-aws-security-center-and-securitywhitepaper/ , published June 2009.
[11] Jinesh Varia, Amazon Web Services, "Building GrepTheWeb in the Cloud, Part 1: Cloud Architectures", Available: http://developer.amazonwebservices.com/connect, July 2008, pp. 1-7.
[12] Jon Brodkin, " Gartner: Seven Cloud-Computing Security Risks", Available: http://www.infoworld.com, published July 2008, pp. 1-3.
[13] Amazon White Paper, "Introduction to Amazon Virtual Private Cloud", Available: http://aws.amazon.com/about-aws/whatsnew/2009/08/26/introducing-amazon-virtual-private-cloud/ , published Aug 26, 2009, pp. 6-8.
[14] L. Zhou, V. Varadharajan, and M. Hitchens.Enforcing role-based access control for secure data storage in the cloud.The computer Journal, 2011
[15] American National Standard for Information Technology: Role -based access control. ANSI INCITS 359- 2004(2004)
[16] Arshad, J. Townend, P. Jie Xu , "Quantification of Security for compute Intensive Workloads in Clouds", 15th International Conference on Parallel and Distributed Systems, School of Computation, pages 478-486, Dec. 2009, UK.
[17] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning. Managing security of virtual machine images in a cloud environment. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96. November 2009.
[18] Miranda Mowbray, Siani Pearson. A Client-Based Privacy Manager for Cloud Computing. COMSWARE '09: Proceedings of the Fourth International ICST Conference on COMmunication System. June 2009
[19] Flavio Lombardi, Roberto Di Pietro. Transparent Security for Cloud. SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415. March 2010. International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org
[20] A. Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009
[21] D. Gollmann, "Securing Web Applications", Information Security Technical Report, vol. 13, issue. 1, 2008



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY