www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Data security using device Identification in Cloud Platforms by API

[1]Praveen kumar A, [2]Arjunan K, [3]Pavithra M, [4]Usharani M, [5]Vimal R.Y, [6]Vanathi D, [7]Satheeshkumar S
[1-5] Student Department of Computer science and Engineering, Nandha Engineering College, Erode - 052
[6]Associate Professor,Department of Computer science and Engineering, Nandha Engineering College, Erode - 052
[7]Assistant Professor,Department of Computer science and Engineering, Nandha Engineering College, Erode – 052

Email id: apraveenkumar1197@gmail.com, arjunan.k.s.a.t@gmail.com, vimalyogarajan15@gmail.com

Abstract—**Cloud computing is a new computing model that offers a number of advantages such as low cost, only pay for selected services, hardware and software on rent. Due to its increasing popularity in information technology market, many new service providers are trying to implement this new model to provide number of services to Small and Medium Enterprises (SMEs). Hence these models can be used in increasing the security towards the data transmission. This paper was presented from survey findings to overcome the security threads in the data transmission and device identification. This helps the developers to use it as Library or API to increase the security for the system.**

I. INTRODUCTION

Cloud computing is a result of decades of research in virtualization, distributed computing, Grid computing, utility computing and also involves work on networking, web and software services. It implies a service -oriented architecture, reduced IT overhead for the end user.It can be well used provided security issues are not gone to a major concern. It can be used in the protection of data security in network streams. As these data can be encrypted in the manner are decided by the Cloud Platforms.

In general, cloud computing architecture is divided into two layers: the bottom resource layers and the upper service layer. The bottom is the foundation, is based on virtualized resources in the form of storage and computing, the upper service layer to provide specific services. The encrypted data can be prevented from Spoofing attack, Man in the Middle attack etc.;

Initially, this papers specifies the research papers of privacy preserving issues of data using cloud computing, then gives data integration issues and discusses some improvements in new techniques for cloud computing.

II. SECURITY ASPECTTS TO FOCUS ON CLOUDCOMPUTING

The popularity of Cloud Computing is mainly due to the fact that many enterprise applications and data are moving into cloud platforms; however, lack of security is the major barrier for cloud adoption .Many of the threats found in existing platforms. Out of them, the Security Threat is considered to be of High Risk. These threats can be avoided in an application by introducing some suitable elements. They are further explained below:

2.1 Confidentiality

It is the process of making sure that the data remains private, confidential and restricted from unauthorized users. Data encryption is one of the most popular options of security before pushing the data into cloud. Confidentiality means keeping users' data secret in the Cloud systems. Cloud computing system offerings (e.g., applications and its infrastructures) are essentially public networks. Therefore, keeping all private data of

users' secret in the Cloud is a fundamental requirement which will attract even more users consequently. There are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, encrypting data before placing it in a Cloud may be even more secure than unencrypted data in a local data center; this approach was successfully used by TC3.

2.2 Authentication

Is the mechanism by which the systems may securely identify their users. In authentication the origin of an electronic message or document is correctly identified For Example, Suppose that user ABC sends an electronic document over the Internet to user PQR. However, the difficulty is that user ABC has posed as user XYZ when he sent this document to user PQR. How would user PQR know that the message has come from user ABC, who is posing as user XYZ?

2.3 Authorization

Determines the level of access to system resources attributed to a particular authenticated user The principle of access control determines who should be able to access what .For Example, we can specify that user XYZ can view the records in a database, but cannot update them. However, user PQR might be allowed to make updates as well. Access control mechanism can be used to ensure this. Using cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with cloud providers.

2.4 Availability

The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any place, at any time. Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the Cloud system or applications hosted on it. Many Cloud Computing system vendors provide Cloud infrastructures and platforms based on virtual machines. Amazon Web Services provide S3, EC2 entirely depend on the virtual machines called Xen, and Skytap offers virtual lab management application relaying on hypervisors, including VMware, Xen and Microsoft Hyper- V, and so on. This is the reason due to which Cloud service provider can rend resources *(*e.g., CPU cycles, storage capacity, and memory) from Amazon on demand at the expense of usage in terms of a single unit. Hence, the virtual machine is the essential component to host these services. Virtual machines have the capability for providing on demand services in terms of users' individual resource requirement for a large amount of users.

For a cloud user, service should be available at all time. Whenever a user requests for a cloud service, provider and user has to sign SLA (Service Level Agreement). This defines the terms and conditions and specifications for cloud service. It also includes percentage of time service is available. A cloud user expects a high available service with no or minimal downtime. A cloud provider and its corresponding service are selected based on service availability and business needs.

2.5 Integrity

When the data of a message is modified after the sender sends it, but before it reaches to the intended recipient, then the integrity of a message is lost. In this the data is protected from accidental or malicious modification. Data integrity in the Cloud system is to preserve information integrity (i.e., not lost or modified by unauthorized users). As data is the foundation for providing Cloud Computing services, such as Software as a Service, Platform as a Service, Data as a Service, keeping data integrity is a basic task. Cloud computing system usually provides large data procession capability. Digital signature is a normally used technique for data integrity testing. The widely accepted distributed file systems (e.g., GFS, HDFS) usually divide data in large volumes into a set of blocks, each of which has a default size (e.g., 64MB, 128MB). When a block of the data is physically stored then a digital signature is attached to it. In this digital signature is able to test the integrity of the data, and recover from fraud. Hence, data integrity is basic for Cloud Computing system, and it is achieved by techniques such as RAID-liked strategies, digital signature, hashing techniques, and message authentication codes and so on.

2.6 Non-repudiation

Nonrepudiation is the guarantee that someone cannot deny something.It refers to the ability to ensure that a party to a contract or a communication cannot deny the

authenticity of their signature on a document or the sending of a message that they originated. Repudiation is defined as the denial of an entity of having participated in all or part of a communication. Consider the example: Alice wants to send a message to Bob; after having sent the message, Alice may deny having sent it (repudiation of origin), or Bob may deny having received it (repudiation of receipt). Therefore, specific protocols have been designed in order to generate evidences for non-repudiation of origin (NRO) (for Bob), and non-repudiation of receipt (NRR) (for Alice). In case of a dispute Alice or Bob will present their evidences to an adjudicator, who will take a decision in favor of one of the two entities without ambiguity

2.7 Privacy

Privacy is a crucial issue for cloud computing, each in terms of legal compliance and user trust and this need to be considered at every phase of design. The important consideration for software engineers while designing the cloud services in such a way as to decrease privacy risk and to ensure legal compliance.

Loss of governance: A cloud provider site is located in onecountry and the cloud user may be using the service from different country. User data which is stored from one country is owned and is under the control of cloud provider country, its misuse may have a significant impact on privacy, security and intellectual property claims.*Regulatory compliance:* Regulated data may reside in thecloud, the obligation for regulatory compliance may still falls with the organization that owns the data.*Lack of transparency:* Cloud vendors do not alwaysdisclose the details of how their services work, which third-party partners they use, and exactly where data is located. The information about the user data, security measures etc. are generally not known to user.Cloud system designers, architects, developers and Testers must consider the following points

1. Minimize personal information sent to and stored in the cloud.
2. Protect personal information in the cloud.
3. Maximize user control.
4. Allow user choice.
5. Specify and limit the purpose of data usage.

2.8 Control

Control within the Cloud Computing System means to regulate the use of the system, including the applications, its infrastructure and the data .Cloud computing system involves large–scale data sets & that are distributed across multiple number of computer nodes. Every Internet user is able to contribute his or her individual data to the Cloud Computer systems which are located on the other side of the Internet, and make use of them. Future healthcare applications may use an individual's DNA sequence (which is captured by hospitals) to develop tailored medicine and other personalized medical treatments. When all these private data are stored in the Cloud Computing system environment, users of Cloud Computing systems may face many threats to their individual data. Hence, economical and effective control over the data access within the Cloud Computing system and regulate behaviors of the applications (services) hosted on the Cloud Computing systems can enhance the safety of systems.

2.9 Audit

Audit is a programming approach to watch what happened in the Cloud system. It could be added as an additional layer above the virtualized operation system hosted on the virtual machine to provide facilities for watching what happened in the system For such kind of scenarios, the state changes and other factors that effected the system availability should be audited· Such a new feature reinforces the Cloud Computing developers to focus on providing virtualized capabilities instead of specific hardware to being provided. Another related thing is that many nations have laws requiring Cloud Computing providers to keep customer data and copyrighted material within national boundaries, which make the auditability hopefully in the law issue perspective.

2.10 Compliance

Compliance can help prepare CSPs (Cloud Service Provider) and their users to address rising requirements. To drive efficiency, risk management, and compliance, CSPs need to implement an internal control monitoring function together with a robust external audit process. In order to gain comfort over their in-cloud activities, CSP users need to define their control requirements, understand their CSP's internal control monitoring processes, analyze relevant external audit reports, and

properly execute their responsibilities as CSP users.

2.*11 Security-as-a [cloud] Service*

Security-as-a-service is having important future growth because of two reasons. First, a continues shift in data, because of which security work will continue from in-house to outsource. Second, several other information security needs are present for organizations currently, but they will accelerate in need and complexity with the growing adoption of cloud computing. The two proactive controls are important to the growth of cloud computing: identity management that is inter-cloud and scalable to the cloud size, and (encryption) key management.

The two reactive controls are required for audit and compliance purposes as well: scalable and effective SIEM, and data leakage prevention (DLP). Providing solutions to these controls will be difficult and are complex one that must be hugely scalable and yet easy to use.

III. UNITS

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage**.** For example, write "15 Gb/cm^2 (100 Gb/in^2)." An exception is when English units are used as identifiers in trade, such as "3½-in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength *H* is A/m. However, if you wish to use units of T, either refer to magnetic flux density *B* or magnetic field strength symbolized as $\mu_0 H$. Use the center dot to separate compound units, e.g., "A·m^2."

3.1 Threats to cloud computing discovered by "Cloud Security Alliance" (CSA)

Cloud Security Alliance is a well-known community relegated to cloud security. It has proposed the security threats of cloud systems. These threats are illustrate as follows:

3.1.1 Abuse and Nefarious Use of Cloud Computing

This threat is relating to the shortcomings of registration process associated with cloud. Cloud Service Providers offer IAAS and PAAS to their customers with a minimum requirement of a credit card. By taking advantage of this registration process, hackers may be able to conduct susceptible activities like Spamming and Phishing. Initially, PAAS providers have suffered from this attack. However, recent evidence shows that hackers have begun to target IAAS vendors as well (CSA-Cloud Security Alliance).

3.1.2 Insecure Application Programming Interfaces

Software interfaces or APIs are used by customers to interact with cloud services, which must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

Cloud providers provide a set of software interfaces or APIs that customers use to manage and interact with the cloud services. The security and availability of cloud services depend upon the security of these basic APIs. Without proper management of authentication, it leads to Insecure Interfaces. To maintain the secrecy of cloud data, the interfaces must be designed to protect against both accidental and malicious attacks.

3.1.3 Malicious Insiders

Malicious insider, working as a cloud employee, collecting confidential data or taking complete control of the cloud services with minimal or no possibility of detectionNentwich, N. Jovanovic. Therefore it is a important challenge as to how an organization can restrict its internal employees, contractors, vendors and other trusted people who have access to critical resources from within the network. This key challenge can be addressed to a certain degree by enforcing strict supply chain management and conducting a comprehensive supplier assessment. Authorization plays a important role in securing the cloud.

Transparency is very important in the information security and management. When a cloud provider hires their cloud employees, certain factors such as hiring standards, policies regarding how their employees can access to virtual & physical assets and how the

employees are being monitored in their work are to be clarified.

If the cloud provider does not consider the significance of the above factors, this situation may create more opportunities to the hackers.

3.1.4 Shared Technology Vulnerabilities

Sharing infrastructure is a life for IaaS providers. These infrastructures were not designed to offer strong isolation. Strong compartmentalization is required to ensure that users do not interfere with other tenants running on the same cloud provider. Thus, compromise on Confidentiality is a serious security issue.

3.1.5 Data Loss/Leakage

Top threats for Cloud Computing like Data loss or Data leakage may due to how the data is structured. Firstly, data of an organization must be stored in servers of other nations. This is a significant concern for some organizations. Secondly, the duration of data retained by the Cloud provider, may continue to remain on the provider's servers, even after it has been deleted by the client. Thirdly, improper deletion of data records and alteration of data without proper backup can result in permanent loss of data. Last but not the least, insufficient authentication, authorization and audit control, allows unauthorized parties to gain access into sensitive data. Therefore, Data Integrity must be upheld if CC is to be secured.

3.2 Security Problems Concerning Location of the Cloud Systems

Some problems are inherited from the specific features of cloud computing. In cloud computing system, data storages are spread around the world. This may result in some security problems as bellow:

3.2.1 Multi-location of the private data

The businesses' private data are residing on someone else's computer and in someone else's facility which is dangerous. Many things can be wrong with the data such as the Cloud service provider may go out of business. Secondly, the Cloud service provider may decide to hold the data as hostage if there is a dispute.

3.2.2 Multi-location of the service provider

The Cloud service clients it may be business user or private user also need to make sure that how the Cloud service provider performs their declared services.Thus, in this way the Cloud service client is able to keep a direct relationship with the Cloud Service provider, and control its own private data.

3.2.3 Data combination and commingling

The Cloud Computing client such as business user or private user must ensure that whether its private data is stored separately from others or not. If they are combined or commingled with other clients' data, then it is much more dangerous. If another client is the victim of a hack attack, the attack might affect the availability or integrity of the data of other clients located in the same environment. For example, viruses might be transmitted from one client to others.

3.2.4 Restrictions on techniques and logistics

It might be very difficult or even impossible for the Cloud service provider to assure the locations where theCloud Computing client's data will be stored. Consider the example, Amazon has data centers that are all over the world; the client's data is placed automatically across them, unless Amazon uses specific servers for dedicated client. The Cloud service provider may also need to address logistics. Cloud computing providers needs to delegate the data hosting or other service to third parties.

3.2.5 Data transfer across the borders

Knowing where the Cloud service supplier will host the data may be a requirement to know the way to transfer data across the country borders. As a result of multi-locations of the 3 parties within the Cloud Computing scheme i.e. Cloud supplier, XaaS Cloud user/provider, XaaS user, the data request storage and the processing sometimes conduct in numerous countries or places, that build the laws to be applied even additional complex, and because of which the private information to be even additional vulnerable from attack.

3.3. Cloud Challenges Inherited From Network Concept

Cloud computing mainly depends upon internet and remote computers or servers in maintaining data for running various applications. The network is used to

upload all the information. The network structure of this cloud faces various attacks and security issues which are explained further below.

3.3.1 SQL injection attacks

In this type of attack a malicious code is inserted into a standard SQL code. Thus the attackers get unauthorized access to a database and are able to access sensitive data.

Further, SQL injection attacks as described by Sara Quasar et al. [18], uses the special characters to return the data for example in SQL scripting the query usually ends up with where clause which again may be modified by adding more rows and information in it. The information entered by the hacker is misunderstand by the website as that of the user's data and this will then allow the hacker to access the SQL server leading the invader to easily access and modify the functioning of a website.

3.3.2 Cross Site Scripting (XSS) attacks

In this attack injecting malicious scripts into Web is done. There are two methods for injecting the malevolent code into the web-page that is displayed to the user: Stored XSS and Reflected XSS. In case of Stored XSS, the malicious code is permanently stored into a resource managed by the web application. However in case of a Reflected XSS, the attack script is not permanently stored; in fact it is immediately reflected back to the user P. Vogt

3.3.3. Man in the Middle attacks (MITM).

In this attack, an entity tries to interrupt an ongoing conversation between a sender and a receiver to inject false information and to have knowledge of the important information transferred between them. Various such as Airjack , Cain ,Dsniff, , Ettercap, Wsniff, etc. have been developed for providing protection against these attacks.

3.3.4 Sniffer Attacks

These attacks are launched by applications which can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, then it can be read. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded.

3.3.5 Reused IP Addresses

When a particular user moves out of a network, then the IP-address associated with him earlier is assigned to the new user. Even if the old IP address is being assigned to a new user, the chances of accessing the data by some other user is not less as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user abuse the privacy of the previous user.

3.3.6 Denial of Service Attacks

This attack prevents the consumer from receiving the service from the cloud.It usually floods the cloud with excessive requests to the target server and the actual consumer might not be able to receive the service since the server is busy servicing the attacker. There are many methods to perform a DoS attack such as SYN flood. A SYN flood use the TCP 3-way handshake by requesting connections to the target server and ignoring the acknowledgement (ACK) from the server. This makes the server to wait for the ACK from the attacker, wasting time and resources. Because of which, the server does not have enough resources to provide services to clients. This attack can be prevented by authorizing strict access to the cloud and using cryptographic protocols to ensure that the right personnel are accessing the cloud.

If an attacker intercepts the SOAP message and modify the receiver's e-mail address to the attacker's e-mail address, the web service will forward the e-mail to the attacker.

3.3.7 Xml signature element wrapping

As clients are typically able to connect to cloud computing via a web browser or web service, the web service attacks also affect cloud computing. XML signature element wrapping is the eminent attack for web service. Although Cloud security uses XML signature in order to protect an element's name, attributes and value from unauthorized parties, it is unable to protect the particulars in the document. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value

the attacker would like and moving the original element to somewhere else on the SOAP message. This method can trick the web service to process the malicious message created by the attack. Figures 5 and 6 illustrate an example of an XML signature element wrapping attack. As per the figure 5, the client requests a picture called "me.jpg". However, if the attacker intercepts and alters the SOAP message by inserting the same element as the client but the attackers requests a document named "cv.doc" instead of the image shown as the figure 6. After the web service receives the message, the web service will send the document back to the client. Another attack may be in the case of the e-mail web service application.

3.3.8 Browser Security

Every client uses browser to send the information on network. The browser makes use of SSL technology to encrypt user's identity and credentials. But hackers from the intermediary host may acquire these credentials by the use of sniffing packages installed on the intermediary host. Steve Kirsch [20] states that in order to overcome this, one should have a single identity but this credential must allow various levels of assurance which can be achieved by obtaining approvals digitally. Moreover, M. Jensen, has shown that Web Services security (WS-security) concept on browsers work with XML encrypted messages which does not need to be decrypted at intermediated hosts.

3.3.9 CAPTCHA Breaking

Recently, it has been found that the spammers are able to break the CAPTCHA [22], provided by the Hotmail and Gmail service providers. They use audio system to read the CAPTCHA characters for the visually impaired users. Various methods such as: variable fonts of the letters used to design a CAPTCHA, implementing letter overlap, increasing the string length and using a perturbative background can be used to avoid CAPTCHA breaking [23]. Single frame zero knowledge CAPTCHA design principles have been proposed, which will be able to oppose any attack method of static optical character recognition (OCR).

3.3.10 Cookie Poisoning

Cookie poisoning involves changing or alerting the contents of cookie to have an illegal access to a webpage or an application. Basically cookies contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be copied to masquerade as an authorized user. Figure bellow explain this kind of attack.

3.4. Cloud Threats Inherited From Virtualization

Virtualization is yet another important technology for the realization of CC; but the services provided by Virtualization may also introduce some forms of risks to its applications Flavio Lombardias explained below:

3.4.1 Isolation Failure

One of the major benefits of Virtualization is Isolation. This benefit, if not deployed properly will generate a threat to the environment . Poor isolation or inappropriate access control policy which will cause the inter-attack between two VMs or between VMs and its associated VMM. For instance, VM Escape is one of the worst cases happening if the Isolation between the host and the VMs is compromised. In case of VM Escape, the program running in a VM is able to bypass the VMM layer and get access to the host machine. Since the host machine is the root of security of a virtual system, the program which gains access to the host machine can also gains the root privilege

3.4.2. Dependency on Secure Hypervisor

If a hacker is able to get control over the hypervisor, he can do the changes to any of the guest operating systems and get control over all the data passing through the hypervisor. Based on the understanding of how the various components in the hypervisor architecture behave, an advanced cloud protections system can be developed by monitoring the activities of the guest VMs (Virtual Machines) and inter-communication among the various infrastructure components.

3.4.3. Multi-tenancy

During execution of multiple VMs on the same host, different users can share both the application and physical hardware ShengmeiLuo. This may lead to information leakage and other exploitations. For instance, in a virtual system, improper VM management policy will cause VM sprawling, a case where number of VMs increasingly growing while most of them are idle or never be back from sleep, which may cause

resource of host machine being largely wasted.

3.4.4. VM Hopping

In VM hopping, an attacker on one VM gains rights to use another victim VM. The attacker can check the victim VM's resource procedure, change its configurations and can also delete stored data, thus, putting it in danger theVM's confidentiality, integrity, and availability. A requirement for this attack is that the two VMs must be operating on the same host, and the attacker must recognize the victim VM's IP address.

3.5. Device Identification

The Unique Device Identification (UDI) System is intended to assign a unique identifier to medical devices within the United States. It was signed into law on September 27, 2007, as part of the Food and Drug Administration Amendments Act of 2007. This act includes language related to the establishment of a Unique Device Identification System. When implemented, the new system will require:

- The label of a device to bear a unique identifier, unless an alternative location is specified by the U.S. Food and Drug Administration (FDA) or unless an exception is made for a particular device or group of devices.
- The unique identifier to be able to identify the device through distribution and use
- The unique identifier to include the lot or serial number if specified by FDA

A national UDI system will create a common vocabulary for reporting and enhance electronic tracking abilities. Currently, analysis of adverse event reports is limited by the fact that the specific devices involved in an incident are often not known with the required degree of specificity. Without a common vocabulary for medical devices, meaningful analysis based on data from existing voluntary systems is problematic. Reliable and consistent identification of medical devices would enable safety surveillance so that the FDA and manufacturers could better identify potential problems or device defects, and improve patient care. The UDI is expected to improve patient safety (in part by helping to identify counterfeit products and by improving the ability of staff to distinguish between devices that are similar in appearance but serve different functions), facilitate and improve the recall process, and create efficiencies within the medical system.

In the most basic format, the UDI would be a coded number registered with standards organizations, and would incorporate a variety of information, including (but not limited to) the manufacturer of the device, expiry dates, the make and model of the device, and any special attributes that the device may possess. In a medical sense, "device" refers to any product that is not pharmaceutical in nature, and while the FDA have been given approval to exempt some devices, Jay Crowley (who was responsible for implementing the UDI requirements in the Act), has expressed an intent to apply the UDI to "everything until somebody gives us good reason not to", (excluding devices which won't need identification).Following the passing of the Act, there were calls for the FDA to publish a timeline for the implementation of the UDI; this was subsequently done.GUDID Submission the Final Rule on Unique Device Identifiers also mandates medical device manufacturers to make a submission to the FDA's Global Unique Device Identification Database. The submission to the GUDID will include the Primary Device Identifier portion of the UDI as well as associated data attributes about each model or version number of the device. Compliance with the submission component of UDI compliance is phased according to the Class of device. Class III device labelers must submit to the GUDID for all existing products by September 24, 2014. Labelers of Implantable, Life Supporting or Life Sustaining devices must submit to the GUDID by September 24, 2015. Class II labelers must comply with submission guidelines by September 24, 2016, and Class I labelers by September 24, 2018.Submission to the GUDID may be made in one of two methods. The first method utilizes the FDA's GUDID Web Interface, which is meant for low volumes of GUDID submissions. The second method utilizes an HL7 SPL submission and is transmitted to the FDA through an Electronic Submission Gateway account.Although PaaS and IaaS users have partial authority, Thomas Ristenpart et al. have shown that an attacker can get hold of or decide the IP address using benchmark customer capabilities on the basis of various tricks and combinational inputs to fetch user's IP.Additionally, multi-tenancy makes the impact of a VM hopping attack larger than in a conventional IT environment. Because quite a few VMs can run at the

same time and on the same host there is a possibility of all of them becoming a victim VMs. VM hopping is thus a serious vulnerability for IaaS and PaaS infrastructures.

IV.CONCLUSION

Any application relying upon an emerging technology should consider the different possible threats. Such an application with an inability to anticipate or handle the threats may probably lead to failures. The classification of various security threats/issues presented in this paper would definitely benefit the cloud users to make out proper choice and cloud service providers to handle such threats efficiently.

REFERENCES

[1] Ramgovind S, Eloff MM and Smith E, "The Management of Security in Cloud Computing", IEEE, 2010

[2] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z; (2010),"Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105, 1-3 Nov. 2010.

[3] Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues, "Towards Trusted Cloud Computing", Conference on Hot Topics in Cloud Computing 2009, pages 1-5, USA.

[4] Hyukho Kim, Hana Lee, Woongsup Kim, Yangwoo Kim, "A Trust Evaluation Model for QoS Guarantee in Cloud Systems", International Journal of Grid and Distributed Computing, March, 2010.

[5] Zhimin Yang at el, "A Collaborative Trust Model of Firewall-through based on Cloud Computing", 14th International Conference on Computer Supported Cooperative Work in Design, 2010, China

[6] Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE/IFIP International
Conference on Embedded and Ubiquitous Computing, 2010, Australia

[7] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, MateiZaharia. A view of cloud computing. *Communications of the ACM , Volume 53 Issue 4*, pages 50-58. April2010.

[8] Siani Pearson. Taking Account of Privacy when Designing Cloud Computing Services. *CLOUD '09: Proceedings of the 2009 ICSEWorkshop on Software Engineering Challenges of Cloud Computing*, pages 44-52. May 2009

[9] Tim Mather, SubraKumaraswamy, ShahedLatif Cloud Security and Privacy : An Enterprise perspective of Risks and Compliance, O'Reilly Media, Inc., 2009

[10] Bansidhar Joshi, A. SanthanaVijayan, Bineet Kumar Joshi, "Securing Cloud computing Environment against DDoS Attacks", IEEE, 2011, pp. 1-5.

[11] HaoyongLv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, 2011, pp. 214-216.

[12] AmanBakshi and Yogesh B, "Securing cloud from DDOS Attacks using Intrusion Detection System in VM", IEEE, 2010, pp. 260-264.

[13] PrashantSrivastava, Satyam Singh, Ashwin Alfred Pinto, ShvetankVerma, Vijay K. Chaurasiya and Rahul Gupta, "An architecture based on proactive model for security in cloud computing", IEEE, 2011, pp. 661-667.

[14] QinboXu, Cuixia Ni, Guang Jin, and Xian Liang, "Improve the information security practice Instruction with VM techniques", IEEE, 2010, pp. 285-288.

[15] AkhilBehl, "Emerging Security Challenges in Cloud computing, an insight to Cloud security challenges and their mitigation", IEEE,
2011, pp. 217-221.

[16] Yoshiaki Hori, Takashi Nishide and Kouichi Sakurai, "Towards Countermeasure of Insider

Threat in Network Security", IEEE, 2011, pp. 633-636.

[17] S. Ghemawat, H. Gobioff, and S. Leung, "The Google file system," in *Proceedings of the 19th Symposium on Operating SystemsPrinciples (OSDI'2003)*, 2003, pp. 29–43.

[18] Sara Qaisar, KausarFiazKhawaja, "Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329.

[19] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross-Site Scripting Prevention with Dynamic Data

[20] Tainting and Static Analysis", Proceedings of the Network and Distributed System

[21] Steve Kirsch et al., "The Future of Authentication", 1540-7993/12, IEEE, January-February 2012, pp: 22 – 27.

[22] M. Jensen, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, pp: 109 – 116.

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

[24] Albert BJeng, Chien Chen Tseng, Der-Feng Tseng, Jiunn-Chin Wang, "A Study of CAPTCHA and its Application to User Authentication", Proc. Of 2nd Intl. Conference on Computational Collective Intelligence: Technologies and Applications, 2010.

[25] UdayaTupakula and Vijay Varadharajan, "TVDSEC: Trusted Virtual Domain Security", IEEE, 2011, pp. 57-63.

[25] ShengmeiLuo, Zhaoji Lin, Xiaohua Chen, "Virtualization security for Cloud computing service", IEEE, 2011, pp. 174-178.

[26] JyotiprakashSahoo, Mohapatra and Lath R, "Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues", IEEE, 2010, pp. 222-226.

[27] Jenni Susan Reuben, "A Survey on Virtual Machine Security", Seminar of Network Security, Helsinki University of Technology, 2007.

[28] 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.

[29] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing", 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010

[30] HaoyongLv and Yin Hu, "Analysis and Research about Cloud Computing Security Protect Policy", IEEE, 2011, pp. 214-216.

[31] Thomas Ristenpart et al., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS09), ACM Press, 2009, pp. 199–212