CLOUD SECURITY RELATED THREATS

Vaishali Singh, S. K. Pandey

Abstract— Successful implementation of Cloud Computing architecture requires proper planning and understanding of emerging risks, threats, vulnerabilities and their possible countermeasures. Cloud is transforming the way, computing technology and applications are being designed and delivered but at the same time, these advances have created several new issues whose full impact is still emerging. Security is one of the major issues, which is hampering the growth of Cloud Computing as there is lack of commonly accepted set of standards, policies, processes, and practices. The absence of these aforementioned aspects tends to make the cloud vulnerable to security breaches and thus is an emerging area for study. The goal of this paper is to identify the major security threats and to draw the attention of both decision makers and users to the potential risks of moving data into "the cloud" due to these identified threats.

Index Terms — Cloud Security, Threats, Cloud Computing, Security Threats, Information Technology, Security, Cloud Computing Security, Cloud Threat

1. INTRODUCTION

The emergence of Cloud Computing has drastically altered everyone's perception of infrastructure architecture, software delivery and development models. Cloud Computing is a model to enable suitable, on-demand network access to a mutual pool of configurable computing resources [1]. Protruding as an evolutionary footstep, following the evolution from mainframe computers to client/server deployment models, Cloud Computing comprehends elements from grid, utility and autonomic computing, into innovative deployment architecture [11].

This technology promises to release the client from the burden of administering more and more complex and expensive systems by offering things less than the possibility of using systems with state-of-art computing capabilities, high availability and scalability. It is beneficial for all large enterprises to entrepreneurs, start-ups, medium companies and small companies as it provides enhanced collaboration, agility, scaling and availability and opportunities for cost reduction through optimized and efficient use of computing resources. 56% of European decision-makers estimate that the Cloud is a priority between 2013 and 2014 [2]. But, still Cloud Computing adoption and diffusion are threatened by unresolved security issues that affect both the Cloud provider and the Cloud user.

- Vaishali Singh, 1 Department of Computer Science, St. Xavier's College, JAIPUR -302001, INDIA, vaishali.siingh@gmail.com
- S. K. Pandey, Department of Information Technology, Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament), NOIDA – 201309, INDIA, santo.panday@yahoo.co.in

Cloud Computing benefits can majorly be emphasized to infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of Cloud resources to real needs, improved productivity, but is vulnerable to threats.

Adoption of a cloud service also depends on sharing of responsibilities among the service provider, the customer and is surrounded by many security issues as reliability, availability of services and data, complexity, costs, performance, migration, reversion, regulations and legal issues and the lack of standards [3]. As Cloud gains popularity, it is likely that more criminals find new ways to exploit system vulnerabilities like applying Denial of Service (DoS) on the same environment where other users' resources are being hosted. Many underlying risks and challenges increase the threats in a Cloud Computing environment. Breach in the security of any component in the Cloud can be disastrous for the organization (the customer), will deface the provider and can also quickly erase gains made by switching to this computing technology.

Attacks like SQL Injection, XPath Injection, cookie manipulation and others, which aim to hamper the database, web service and other necessary parts of cloud pose a great threat to cloud system [31]. This paper explores significance security threats related to Cloud Computing focusing on threats specifically related to the shared, on-demand nature of the cloud. The paper emphasis on creating awareness and protect the users from the impact of threats in the Cloud Computing so that the organization or user believes in Cloud technology with trust and trusted security polices as well.

Beyond this introduction on the background details, the remainder of this paper is organized as follows. The section II highlights the Cloud Computing Security. Afterwards, major security threats are given in the section III. Finally, Conclusion and the Future Work are reported in section IV.

2. CLOUD COMPUTING SECURITY

Security is considered as a key requirement for Cloud Computing [28]. Some crucial security and legal obstacles for Cloud Computing include service availability, data confidentiality, provider lock-in and reputation fate sharing

[29]. While the catastrophe arises with the source of origin of the cloud computing technologies which is composite of features like Resource distribution, scalability, Virtualization which tends to produce disasters which is prone to ultimate data leakage and other vulnerabilities [30].

Cloud is being rapidly used by companies to reduce costs, increase flexibility but as more data, applications and infrastructure move to the Cloud, security remains a top fear. With the extensive use of virtualization, more concern has shifted towards security for the public Cloud as security processes that were once visible are now concealed behind levels of abstraction. This lack of visibility creates a number of Cloud Security issues [19]. The Cloud users need to maintain Confidentiality, Privacy, Reliability and Integrity. So, better security policies, processes and best practices are needed for the Cloud.

Cloud security is essentially about the protocols, methodologies and technologies that look after the resources and maintain the veracity of data stored in a Cloud Computing system [4]. User's authentication and authorization, up-time and performance, data backup, disaster recovery and reliable SLAs for Cloud are some of the practices that cloud providers should perform to increase the Cloud adoption rate. Knowledge about the cloud security threats is the first step to prevent them from fear [19]. A malicious insider creates threats which basically target the Cloud providers through hijacking an infrastructure or the services provided and also through exploiting service interfaces. For an example, MITM (Man-In-The-Middle) attacks such as session hijacking and MAC (Media Access Control) spoofing are some of the critical threats for wireless networks.
Increase in use of cloud computing appeals more criminals to find new ways to exploit vulnerabilities which lead to new challenges and risks for the system and thus increase the threat. Agencies like Advanced Persistent Threat (APT) programs identify the one who exactly is behind any attack launched. Another such agency is threat intelligence, which works on the touchstone defences for Cloud organizations that are at risk of being attacked. Aiming to concentrate and organize information related to Cloud security and to facilitate future studies, in this paper we try to identify the main problems in the area through this paper.

3. SECURITY THREATS

The promising technologies appear to sustain, and insist the adequate level of security assurance in software projects. There is no doubt that security is now a 'vibrant burning issue'. It needs to address significantly and no escape is possible [33]. In IT industries, security is considered as wheels that drive the entire system very smoothly. A variety of techniques have been deployed systematically or strategically for developing secure software, but still attackers are incessantly exploiting vulnerabilities [34]. Existing security technology controls could be constrain to minimize persistent threats but still the complete security awareness could be provided by the change towards the behaviour of the people undertaking its use [35].

Cloud Security is being a constant issue for Cloud Computing. For the adoption of Cloud, lack of security is the major problem. This has lead to an increase of issues and challenges for the Cloud. This paper identifies the, major security threats in Cloud Computing. Cloud security threats are identified and classified into different categories. These threats are given as follows [5] [6] and also shown in Fig. 3.1.

3.1 Data Breaches

A data breach is an unpleasant incident with confidential data, which has been viewed potentially by an unauthorized individual [21]. In simple words, when an attacker hacks into a mutual network to filch sensitive data, data breaches can easily be seen in Personally Identifiable Information (PII), financial information such as credit card or bank details, Personal Health Information (PHI), Trade Secrets of Corporations. Major threats coming under this category are listed below:

- **Encryption Related Threat**

One of the threats in encryption is that it limits the efficiency of the Cloud services because large data is expensive and time consuming to get encrypted as well as need to be stored before encryption then decrypted in the mean while one can manipulate the data which will lead to violation of data integrity [22].

- **Data Tampering**

An attacker violates the Integrity of data by modifying it in local memory, a data-store, or on the network. Modification of this data could provide the attacker with access to a service through a number of the different methods listed in this document. Data tampering (integrity) often take the forefront of the security discussion when it comes to the Cloud; the accessibility of data should not be overlooked [24].

- **Data Privacy Breach**

Such incidents mainly involve leakage of private information of individuals, i.e. social security numbers, etc. Loss of corporate information such as trade secrets, sensitive corporate information, details of contracts, etc. or government information is frequently unreported, as there is no compelling reason to do so in the absence of potential damage to private citizens. In Cloud where everything is at a single place or centralized systems work such a breach can have huge impact on client data [23].

- **Information Disclosure**

The unwanted exposure of private data is information disclosure. Information disclosure attacks are aimed at acquiring system-specific information about a website such as software distribution, version numbers, and patch levels [15].

- **Token Stealing**

An attacker steals the credentials or token of another user in order to gain authorization to resources or operations they would not otherwise be able to access [31]

3.2 Data Deprivation

Data Deprivation can be viewed as removal of data without a backup, by thrashing of the encoding key or by unauthorized access; data is always in hazard of being lost or stolen. This is one of the top concerns for businesses sector, as

they not only stand to lose their reputation, but also obligated by law to keep it safe [27]. Major threats coming under this category are given as follows:

- **Insecure/Incomplete Data Deletion**

Incomplete data means data being deleted or modified without any backup of the original content. To delete an information to its full, since a storage media such as a hard disk might be shared by multiple organizations. The storage of unlinked data on unreliable media creates unrecoverable data threats [24].

- **Data Loss or Leakage**

Data are stored in servers. A moment or two, it happens that after deletion of information from the Cloud by the user the data lingering is left which can be misused. Many a times it has been seen that the record is not altered or deleted properly as well as there is no backup of data which leads to permanent loss of data. It can be stolen or leaked by the unauthorized user [25].

- **Data Location Threats**

Threats can be generated due to the security problems concerning location of the Cloud systems such as multi-location of the private data, multi-location of the service provider, data combination and commingling, restrictions on techniques and logistics and data transfer across the borders [26].

3.3 Cloud Misapplication

Cloud misapplication threat can be very harmful in centralized and shared systems like cloud; abuse by cybercriminals can take place in many ways and they can go undetected for long. Some such threats are listed below as:

- **Abuse and Nefarious Use of Cloud Computing**

In Cloud Computing, there is no strict registration process, anyone can use credit card and register itself online on Cloud or through free trail services of vendors. This opens a line of approach for nefarious users who exploits the Cloud resources for setting up botnets, spamming, and spreading virus and so on [25]. One can exploit the vulnerabilities and apply DoS on the same environment where other user's resources are hosted. For example an online Cloud based corporate email service & web portal might be vulnerable to SQL Injection & XSS (Cross-site scripting) which when exploited could result in compromise of other corporate information / email hosted in the same environment [7].

- **SQL Injection**

When there is a failure to validate input in cases where the input is used to construct a SQL statement or will modify the construction of a SQL statement in some way. SQL injection attacks can hamper or completely destroy the entire database if someone with right level of access runs a SQL that has been changed intentionally. Such attacks pose a great threat to Cloud based systems as entire database is centralized too [27].

- **Cookie Replay Attacks**

Reusing a previously valid cookie to deceive the server into believing that a previously authenticated session is still in progress and valid. These attacks if successful make the system vulnerable to all kinds of attacks. The security setup in Cloud should be up to date to handle these scenarios which can be common in attacks [31].

- **Cross-Site Scripting (XSS)**

An attacker is able to inject executable code (script) into a stream of data that will be rendered in a browser. The code will be executed in the context of the user's current session and will gain privileges to the site and information that it would not otherwise have [27].

- **XPath Injection**

XPath (XML Path Language) injection can result if the input sent to the Web service is used to influence or construct an XPath statement. The input can bring in unintended results if the XPath statement is used by the Web service as part of some larger action, such as applying an XQuery or an XSLT transformation to an XML document [31].

- **XML Bomb**

XML bomb attacks occur when specific, small XML messages are parsed by a service resulting in data that feeds on itself and grows exponentially. An attacker sends an XML bomb with the intent of overwhelming a Web service's XML parser and resulting in a denial of service attack [31].

- **Cookie Manipulation**

Through various methods, an attacker will alter the cookies stored in the browser. Attackers will then use the cookie to fraudulently authenticate themselves to a service. As cookies are stored on a hard drive and preserve information that allows the applications to validate the user uniqueness, speed up transactions, monitor actions, and personalize content accessible to the user based on identity and preferences. If cookies are compromised it pretence a big risk to the users as well as the Cloud service providers [31].

- **Cross-Site Request Forgery**

Cross-site Request Forgery (CSRF) is said to be interacting with a website on behalf of another user to perform malicious actions. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the complete web applications. A CSRF can be a most important threat in case; the person is Cloud data administrator or a user on the Cloud [31].

3.4 Traffic and Account Hijacking

When an attacker gains admittance to client credentials and can eavesdrop on client activities and transactions, misrepresent data, return distorted information, redirect clients to outlawed sites and compromising with the availability of cloud services, results in judicial proceeding for cloud service providers. Such threats are given bellow as:

- **Spoofing**

It is an attempt to gain access to a system by using a false identity. This can be accomplished by using stolen user credentials or a false IP address. In a Cloud based environment where everything is at a single place or centralized systems work, spoofing is a big threat as in case of

any unwanted happening it will be very difficult to identify the attacker [31].

- **Session Replay**

An attacker steals messages off of the network and replays them in order to steal a user's session. Session IDs facilitate user tracking for a Website and can provide automatic authentication for future visits to that site or associated sites. As session replay attacks do not take place real time they can taken care of by using firewalls, pop up blockers etc [31].

- **Dictionary Attack**

The use of the list of likely used access methods (usernames, passwords, and coding methods) to try and gain access to a system. Dictionary attack is often used by spammers. Dictionary attacks are not often unbeaten against systems that employ multiple-word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals [31].

- **Credential Theft**

Stealing the verification part of an authentication pair (identity + credentials = authentication), like passwords are mostly the only credentials used while entering a web application or a system. If the password or any other forms of credentials that are necessary for logging into a system are compromised it wills pose great risk for the client as well as the provider of the Cloud [31].

- **Network Eavesdropping**

Listening to network packets and reassembling the messages being sent back and forth between one or more parties on the network. Eavesdropping attacks are insidious, because it's difficult to know they are occurring. When connected to a network, user might feed sensitive information which he does not want to like passwords, account numbers, surfing habits, content of email messages - to an attacker which is unknown to them. In a Cloud based environment such attacks make the client vulnerable to attack [31].

- **Canonicalization Attacks**

There are multiple ways to access the same object and an attacker uses a method to bypass any security measures instituted on the primary intended methods of access. Cloud systems that use the Internet to transmit information are sending data packets into the open where they could be discovered by a malicious hacker. Some techniques such as a man in the middle attack could actually intercept packets that contain encryption keys or authentication data. This makes it possible for a hacker to read data, to falsify transmissions and to access services and information within the Cloud [31].

- **Malevolence**

With the lack of transparency, the malicious attackers at the provider's or user's site steal and damage the confidential data through obtaining passwords, cryptography etc., which breaks the trust of Cloud users. It decreases the brand reputation as well as damage the financial value of an organization. So an organization has to restrict its internal employees, contractors, vendors and other trusted people who have access to critical resources from within the network [31].

- **Accounting and Service Hijack**

Account and service hijacking, frequently with stolen credentials, remains a top threat. Stolen credentials, attackers can often admittance decisive areas of deployed Cloud Computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Organizations should be conscious of these techniques as well as frequent resistance in depth protection strategies to contain the damage and possible litigation resulting from a breach [8].

- **Network Threats**

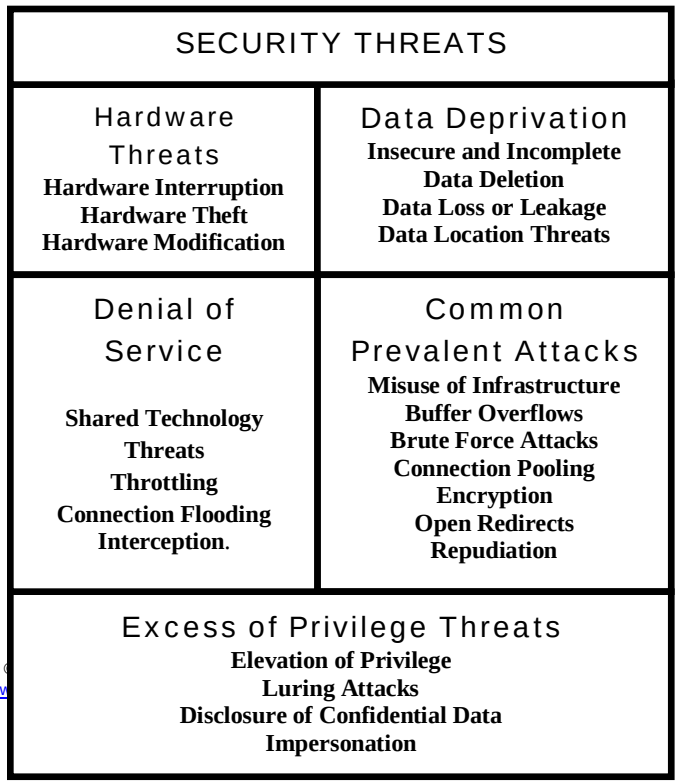
In case of network threats, different threats and attacks has been found such as Man in the Middle Attack (SSL is not properly installed then all the data communication between two parties could be hack by the middle party), Network Sniffing (unencrypted data are hacked through network), SQL Injection Attack (hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information), Cross Site Scripting (user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials) [20].

- **Unknown Risk Profile**

In such case, when an organization undergo any security threat a Cloud provider may not disclose threat due to company's security position and the user is then exposed to unknown risk profile. To find out the company's security position there are some factors which are required to be considered like security practices, vulnerability profiles etc. . [32].

3.5 Hardware Threats

Hardware threats are associated with physical impairment to the routers and switches. One can mitigate hardware threats by providing controlled access to the facilities. The limit access is only network-related to personnel into the Main Distribution Facility (MDF), Intermediate Distribution Facility (IDF), and Network Operations Center (NOC) [18]. Various threats belonging to this category as follows:



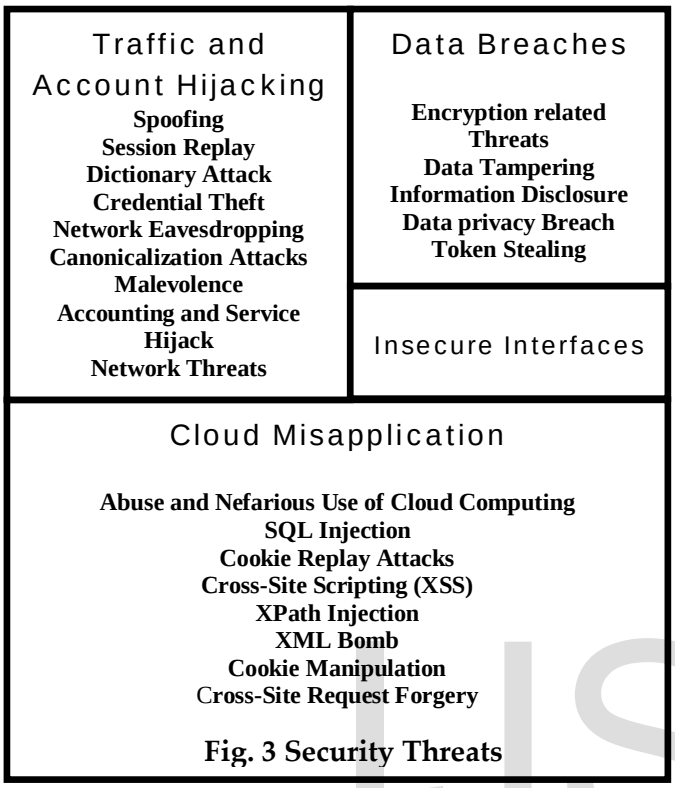


Fig. 3 Security Threats

- **Hardware Interruption**

If one of the applications on a host server is malicious, it might lead to the service provider or some other authority shut down and blocking access the entire server in order to investigate and determine the malicious application [14].

- **Hardware Theft**

Theft at any network setup level can have huge impacts on efficiency n productivity of Cloud. Theft at a data centre can lead to huge losses in terms of both private client data and hardware. In early 2010, Microsoft undertook a survey to assess business leaders' attitudes to Cloud Computing, more than 90 per cent of them were concerned about security and/or of privacy in the Cloud [17] [14].

- **Hardware Modification**

Old n not up to date hardware can lead many run time n compatibility issues between different layers. Though this is the least important layer of the Cloud and often, hardware resources are inexpensive and are not fault tolerant. But the virtualization layer and all layers dependent on the virtualization layer need the hardware layer to be updated [11].

3.6 Excess of Privilege Threats

When the system administrators have inclusive access to servers and its data can pretence a tremendous interior threat if they turn in opposition to the company. System configurations should be locked down so that smallest amount privileges security is being used to reduce the risk of unnecessary privileges being mistreated. The various threats belonging to this category as follows:

- **Elevation of Privilege**

A user with limited privileges assumes the identity of a privileged user to gain privileged access to an application. In various Cloud models elevation of privilege to a user with limited privileges can be a very risk as he may have access to complete database or all software handling or all virtual machines setup [31].

- **Luring Attacks**

An attacker might interest a higher-privileged user to take an action on his or her behalf. It is not an authorization failure but rather a failure of the system which does not properly inform the user. Luring attacks can be pose a danger if it successful in various Cloud models. In infrastructure as a service model if the attacker is able to lure the system to stop virtualization, it will be a big operational risk [31].

- **Disclosure of Confidential Data**

Sensitive data is exposed in some unintended way to users who do not have the proper privileges to see it. Clients main concern over Cloud is security of data and if high standards of user authentication and data security are breached somehow and unauthorized people get access to secured data, it will poses threat for all the Cloud community [31].

- **Impersonation**

It is used to access resources on the same machine where the service code is running. Threats and attacks include: Elevation of privilege- An attacker is able to run in the context of a higher-privileged user. Disclosure of confidential information- An attacker gains access to data that should only be available to another user [31].

3.7 Denial Of Service

Denial of service (DoS) is the process of making a system or application unavailable. For example, a DoS attack might be accomplished by bombarding a server with requests to consume all available system resources, or by passing the server malformed input data that can crash an application process [31]. Distributed- DDoS attack aims to make services or resources unavailable for indefinite amount of time by flooding it with useless traffic [12]. Major threats coming under this category are listed below as:

- **Shared Technology Threats**

Many bugs have been found in all popular VMMs (Virtual Machine Management Service) that allow escaping from VM (Virtual machine). Vulnerabilities have been found in all virtualization software's, which can be exploited by malicious users to bypass certain security restrictions or/and gain escalated privileges. In case of Isolation failure, poor isolation or inappropriate access control policy will cause the inter-attack between two VMs or between VMs and its associated VMM [9].

- **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 privileges. Virtual machines are encapsulated, isolated environments. The operating systems running inside the virtual machine shouldn't know that they are virtualized, and there should be no way to break out of the virtual machine and interact with the parent hypervisor. The process of breaking out and interacting with the hypervisor is called a "VM escape" [10].
- **VM Hijack:** A single server host can host many virtual machines on it with their specific configuration files and security aspects. So the attacker can launch VM Hijack attack on a specific VM and retrieve information.
- **VM Hopping** is an attack which happens, when two VMs are deployed over the same host. One of the sub threats of Virtualization is multi-tenancy, when more than one VM are under execution on the same host, different user share application and physical hardware leads to information leakage.
- **VM Sprawling**, where a number of VMs rapidly growing while most of them are idle or never be back from sleep, which may cause resource wastage.

- **Throttling**

The process of restrictive resource usage to keep a particular process from destroying and/or crashing a system is called throttling. Relevant as a countermeasure, in DoS attacks where an attacker attempts to crash the system by overloading it with input. It is an important step as most Cloud environments run on virtual machines and keeping a check on the process and memory usage by each helps maintain and secure the system from such attacks [31].

- **Connection Flooding**

A flood occurs when a malicious user attempts to attack a network in a variety of evolving ways. The goal of a flood attack is to deplete the victim's resources and disable its services. Flooding attack on the application layer usually makes normal connection with webpage server, and then through browsing behaviours, it wastes the resources of web page, such as CPU time, memory, and bandwidth [16].

- **Interception**

An interception means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. The situation in which, services or data become unavailable, unusable and destroyed. In this sense, denial of service attacks uses maliciously attempts to make a service inaccessible to other parties is a security threat [14].

3.8 Insecure Interfaces

It is sub divided in two parts; Software interfaces or APIs and Management interface compromise. Software interfaces or APIs are used by user to interact with the Cloud services. The security of a Cloud service is embedded in the API of the specific Cloud service. Authentication, authorization, access control, monitoring activities should be implemented to protect against circumvent policy. Value added services also increases risk, so the third party should relinquish their credentials for security [8].

3.9 Other Common Prevalent Attacks

As Cloud Computing is an emerging technology with shared resources and lower cost that relies on pay per use according to the user demand, it faces lots of threats in the scopes of security [27]. We have categorized these threats according to different viewpoints, providing a useful and little-known list of threats. However, there appears numerous threats, which can't be placed any of the aforementioned categories, therefore such type of threats are collected in this miscellaneous category. These are given as follows:

- **Misuse Of Infrastructure**

If Cloud data is moved into a facility that is not equipped to meet regulatory requirements, it will be security breach. Regulatory requirements as, who is legally entitled to have access to my data? What are my legal remedies if something goes wrong? What are my legal remedies in my home jurisdiction if something goes wrong in other jurisdictions? Does the fact that I am storing the data in another jurisdiction subject me to other legal requirements of that jurisdiction? , need to be kept in mind [31].

- **Buffer Overflows**

The maximum size of a given variable (string or otherwise) is exceeded, forcing unintended program processing. These can result in unwanted results from programs or complete program failures. Buffer overflows may become hard to find in complex Cloud enabled services as searching a lone array that has overflow in a complete system may become a tedious task [31].

- **Brute Force Attacks**

The attack which use the raw computer processing power to try different permutations of any variable which could expose a security hole. Brute force attacks have been common from start of computer era and have been used by hackers ever since. These attacks pose a greater threat when it comes to Cloud as a single success over a server can open access to all servers [31].

- **Connection Pooling**

It's a technique to allow multiple clients to make use of a cached set of shared and reusable connection objects providing access to a database [31].

- **Open Redirects**

Attacker provides a URL to a malicious site when allowed to input a URL used in a redirect. This allows the attacker to direct users to sites that perform phishing attacks or other malicious actions. These urls/attacks are direct entry passes for hackers to enter into the system and run malicious code that can hamper anything from hardware to secured data [31].

- **Non Repudiation**

The ability of users (legitimate or otherwise) to deny that they had performed specific actions or transactions is known as repudiation. Without adequate auditing, repudiation attacks are difficult to prove. Logging of each and every event

that takes place in a Cloud based environment is very important in times of high attacks and threats of all kinds [31].

4. CONCLUSION AND FUTURE WORK

Security is an active area of research under the concern of Cloud environment. Little work has been accomplished but still research is going on its various issues. The paper highlights various security threats that currently affects the Cloud system, however there may be some other security threats as well. Research is currently undertaken on the different known threats faced by Cloud systems and possible solutions for the same.

In spite of these research findings, there is an urgent need to work further in the area/s to come up with the novel ideas related to the countermeasures. In this paper, we provided an overview of the major security threats under various categories, which may serve an initial step towards a development of ontology. The paper can provide a significant help to get the research areas, where further work is required especially for entry level researchers.

Future work may be to classify these identified threats with reference to various related parameters. In addition ontology can also be developed to present the findings in more scientific way. Afterwards, the suitable countermeasures may also be developed against each threat to provide adequate security to user and service provider both. The work will have the Cloud Computing to have better confidence as well as trust among the related stack holders.

References

[1] Definition of Cloud Computing. National Institute of Standards and Technology. Access under http://www.nist.gov/itl/Cloud/upload/Cloud-def-v15.pdf.
[2] Challenges & Opportunities for IT partners when transforming or creating a business in the Cloud. compuBase consulting. 2012. p. 77.
[3] Vaishali Singh & S. K. Pandey, "Revisiting Cloud Security Issues and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering Vol.3.Issue7, July-2013, pp. 1-10.
[4] Solar Winds IT Management Glossary, http://www.solarwinds.com/it-management-glossary/what-is-Cloud-security.aspx.
[5] S. Ghemawat, H. Gobioff, and S. Leung, "The Google file system," in Proceedings of the 19th Symposium on Operating Systems Principles (OSDI'2003), 2003, pp. 29–43. http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/de//archive/gfs-sosp2003.pdf [Accessed: 27-05-2013].
[6] JD Meier, Cloud Security Threats and Countermeasures at a Glance, http://blogs.msdn.com/b/jmeier/archive/2010/07/08/Cloud-security-threats-and-countermeasures-at-a-glance.aspx [Accessed: 27-05-2013]
[7] Vishal Kalro, Amit Parekh "Cloud Security & Threat", http://www.chmag.in/article/sep2010/Cloud-security-threat, [Accessed: 29-05-2013].
[8] Cloud Security Alliance "Top Threats to Cloud Computing", http://www.Cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf [Accessed: 27-05-2013].
[9] Nagaraju Kilari , R. Sridaran, "A Survey on Security Threats for Cloud Computing", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 7, September , 2012 pp.1-10.
[10] What is VM Escape? in virtualization, bob plankers, September 22, 2007 , http://lonesysadmin.net/2007/09/22/what-is-vm-escape/ [Accessed: 12-06-2013].
[11] D. Zissis, D. Lekkas, "Addressing Cloud Computing security issues", Future Generation Computer Systems 28 (2012) pp.583–592.
[12] Irfan Gul, Atiq ur Rehman and M Hasan Islam, "Cloud Computing Security Auditing", Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference, IEEE, 21-23 June 2011 pp. 143-148.
[13] Cloud Computing Software, Session-Hijacking, http://www.Cloudcamb.org/software/session-hijacking [Accessed: 14-06-2013].
[14] Security, Introduction to Security, Chapter 8, pp-415, http://www.cs.vu.nl/~ast/books/ds1/08.pdf [Accessed: 16-06-2013].
[15] IBM Security Network Intrusion Prevention System (IPS), Web application protection categories, http://pic.dhe.ibm.com/infocenter/sprotect/v2r8m0/index.jsp?topic=%2Fcom.ibm.ips.doc%2Fconcepts%2Fwap_information_disclosure.htm [Accessed: 16-06-2013].
[16] Chu-Hsing Lin, Chen-Yu Lee, Shin-Pin Lai, Wei-Shen Lai, A Semantic Rule-based Detection Scheme against Flooding Attacks on Cloud Environment, International Journal of Security and Its Applications, Vol. 6, No. 2, April, 2012, pp-341.
[17] Lachlan James, Alice Hutching, Russell G Smith, "Final Report – Cloud Computing Threats Assessment for small business", CEPS, Nov. 2012. http://www.aic.gov.au/media_library/publications/special/002/Cloud-Computing-DBCDE.pdf. [Accessed: 17-06-2013].
[18] Raman Sud and Ken Edelman, "Securing Cisco Routers", CCSP Secur Exam 2 book published by Que, http://searchsecurity.techtarget.com/feature/Securing-Cisco-routers [Accessed: 22-06-2013].

[19] Vaishali Singh & S. K. Pandey, "Research in Cloud Security: Problems And Prospects", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) Vol. 3, Issue 3, Aug 2013, pp 305-314.

[20] Sara Qaisar & Kausar Fiaz Khawaja,"Cloud Computing: Network/Security Threats And Countermeasures", Interdisciplinary Journal Of Contemporary Research In Business, January 2012, Vol 3,No 9, pp.1323-1329.

[21] Top of the Charts in Cloud Risk: Data Breaches By Doug Pollack, February 26, 2013, http://www2.idexpertscorp.com/blog/single/top-of-the-charts-in-cloud-risk-data-breaches/#sthash.s8dayEpx.dpuf.

[22] Dalia Attas and Omar Batrafi, "Efficient integrity checking technique for securing client data in Cloud Computing", International Journal of Electrical & Computer Sciences IJECS-IJENS Vol. 11 No: 05, October 2011.

[23] Vic (J.R.) Winkler, "Cloud Computing: Data Privacy in the Cloud", Adapted from "Securing the Cloud" (Syngress, an imprint of Elsevier), http://technet.microsoft.com/en-us/magazine/jj554305.aspx [Accessed: 22-06-2013].

[24] Snehlata Kothari and Shaloo Dadheech, "Analysis And Enhancing Of Cloud Security Environment", International Monthly Refereed Journal of Research In Management & Technology volume II, February'13, pp 58-66.

[25] Mervat Adib Bamiah & Sarfraz Nawaz Brohi "Seven Deadly Threats and Vulnerabilities in Cloud Computing"(IJAEST) International Journal Of Advanced Engineering Sciences And Technologies Vol No. 9, Issue No. 1, pp.087 – 090.

[26] T.F.M. (Tom) Hendrixen, "Secure Cloud Computing in the Financial Services Market", May 24, 2011, pp.1-64, http://essay.utwente.nl/62877/1/Secure_Cloud_Computing_In_The_Dutch_Financial_Service_Market_v1.0.pdf [Accessed: 18-07-2013].

[27] Vahid Ashktorab & Seyed Reza Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", International Journal of application or Innovation in Engineering & Management (IJAIEM), Volume 1, Issue 2, October 2012, pp.234-245.

[28] IDC (2009) Cloud Computing 2010 – An IDC Update.slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update [Accessed: 20-07-2013].

[29] Mather T, Kumaraswamy S (2009) Cloud Security and privacy: An Enterprise Perspective on Risks and Compliance. 1st edition. O'Reilly Media, Publication Date: October 5, 2009.

[30] Chen Y, Paxson V, Katz RH (2010) What's New About Cloud Computing Security? Technical Report UCB/EECS-2010-5, University of California at Berkeley, eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html [Accessed: 21-07-2013].

[31] "Cloud Security Threats and Countermeasures", JD Meier 8 Jul 2010, http://blogs.msdn.com/b/jmeier/archive/2010/07/08/cloud-security-threats-and-countermeasures-at-a-glance.aspx [Accessed: 22-07-2013].

[32] Sadhana Rana & Pramod Kumar Joshi, "Risk Analysis In Web Applications By Using Cloud Computing", International Journal of Multidisciplinary Research Vol.2 Issue 1, January 2012. Pp.386-394.

[33] S. K. Pandey, S. Rehman, K. Mustafa, S. I. Ahson, "Security Assurance – The Requirements Way", Jan 21, 2008 http://www.cmcrossroads.com/sites/default/files/article/file/2013/Security%20Assurance-The%20Requirements%20Way.pdf [Accessed: 30-07-2013].

[34] S. K. Pandey, K. Mustafa, "Security Assurance by Efficient Non-repudiation Requirements", Advances in Computer Science, Engineering & Applications Advances in Intelligent Systems and Computing Volume 167, 2012, pp 905-912.

[35] C. Banerjee, S.K.Pandey, "Research on software security awareness: problems and prospects", ACM SIGSOFT Software Engineering Notes, Volume 35 Issue 5, September 2010 Pages 1-5.

AUTHORS

Vaishali Singh is presently working as an Assistant Professor in the Department of Computer Science, St. Xavier's College, Jaipur, India. She has an excellent academic background right from the school level. Under the Institute-Industry linkage program, she delivers expert lectures on various areas of Computer Science. She has contributed many research papers in the conferences of national repute. Her research interest includes: Cloud Security, Cloud Security vulnerabilities, threats and countermeasures, Access control, Identity measurement etc.

Dr. Santosh K. Pandey is presently working as a Faculty of Information Technology with Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament) New Delhi. Prior to this, he worked with the Department of Computer Science, Jamia Millia Islamia (A Central University) New Delhi and Directorate of Education, Govt. of NCT of Delhi. He has a rich Academics & Research experience in various areas of Computer Science. His research interest includes: Software Security, Requirements Engineering, Security Policies and Standards, Formal Methods, Cloud Computing, Security Metrics, Vulnerability Assessment etc. He has published around 46 high quality research papers and articles in various acclaimed International/National Journals (including IEEE, ACM, CSI) and Proceedings of the reputed International/ National Conferences (including Springer).

Out of these publications, most of them have good citation records. He has been nominated in the board of editors/reviewers of various peer-reviewed and refereed Journals. In addition, he has also served as a Program Committee Member of several reputed conferences in India as well as abroad. He has also been designated in various academic/research committees by the government organizations as well as software companies as a subject expert.