Security issues in cloud computing: A Study

[1]Amit.V.Kachavimath, [2]Shruti.Somangoudar
[1]Assistant Professor, [2] 6th SEM MCA
Department of Master of Computer Applications,
B.V.Bhoomaraddi College of Engineering & Technology, Hubli, Karnataka, India

***Abstract* - The new developments in the field of information technology offer the people enjoyment, comforts and convenience. Cloud computing is one of the latest developments in the IT industry also known as on-demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. Because of the attractive features of cloud computing many organizations are using cloud storage for storing their critical information. The data can be stored remotely in the cloud by the users and can be accessed using thin clients as and when required. One of the major issues in cloud today is data security. Storage of data in the cloud can be risky because of use of internet by cloud based services which means less control over the stored data. One of the major concern in cloud is how do we grab all the benefits of the cloud while maintaining security controls over the organizations assets. Security controls in Cloud Computing are not different than security controls in IT environment. It is critical for IT Leaders to begin recognizing how these outsourced data service models impact organizational risk. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of security issues involved in cloud computing.**

***Index Terms* - Cloud computing, Data centers, Virtual machines and Secure multi-party computation.**

I. INTRODUCTION

With the significant advances in Information and Communications Technology (ICT) over the last half century, there is an increasingly perceived vision that computing will one day be the utility. This computing utility will provide the basic level of computing service that is considered essential to meet the everyday needs of the general community. To deliver this vision, a number of computing paradigms have been proposed, of which the latest one is known as Cloud computing. Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as telephony. In such a model, users access services based on their requirements without regard to where the services are hosted or how they are delivered. Several computing paradigms have promised to deliver this *utility computing* vision and these include cluster computing, grid computing and more recently *Cloud computing*. The latter term denotes the infrastructure as a "*Cloud*" from which businesses and users are able to access applications from anywhere in the world on demand. Thus, the computing world is rapidly transforming towards developing software for millions to consume as a service, rather than to run on their individual computers. At present, it is common to access content across the internet independently without reference to the underlying hosting infrastructure. This infrastructure consists of data centers that are monitored and maintained around the clock by content providers. Since user requirements for cloud services are varied, service providers have to ensure that they can be flexible in their service delivery while keeping the users isolated from the underlying infrastructure. Recent advances in microprocessor technology and software have led to the increasing ability of commodity hardware to run applications within *Virtual Machines* (VMs) efficiently. VMs allow both the isolation of applications from the underlying hardware and other VMs, and the customization of the platform to suit the needs of the end-user. Providers can expose applications running within VMs, or provide access to VMs themselves as a service (e.g. Amazon Elastic Compute Cloud) thereby allowing consumers to install their own applications

A number of computing researchers and practitioners have attempted to define cloud computing in various ways. Here are some definitions:

- Cloud computing is defined as a pool of virtualized computing resources. Based on this virtualization, the cloud computing paradigm allows workloads to be deployed across physical machines via virtual resources.
- Cloud computing is a model for enabling convenient, on demand on network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- Cloud Computing is a platform or infrastructure in which dynamically scalable resources are provided as a service through internet, enabling users to process the data outside the boundaries of the company, providing economical benefits through virtualized and shared infrastructure without the need of expertise nor knowledge over the underlying technology.

Figure.1 presents an overview of the cloud computing reference architecture, which identifies the major actors, their activities and functions in cloud computing. The diagram depicts a generic high-level architecture and is intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing

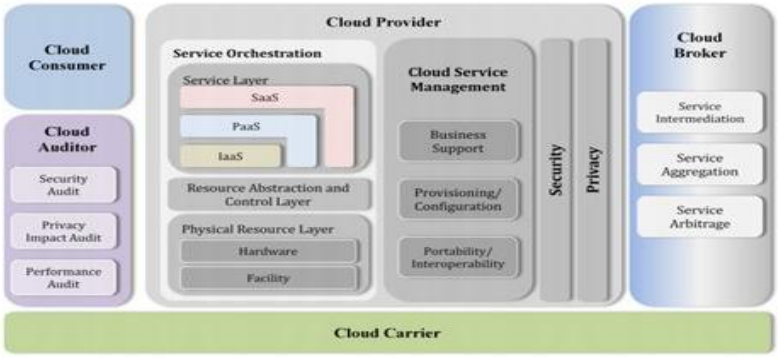

Figure.1

Cloud computing offers numerous advantages both to end users and businesses of all sizes. The obvious huge advantage is that there is no need to support the infrastructure or have knowledge, necessary to develop and maintain the infrastructure, development environment or application, as were things up until recently. The burden has been lifted and someone else is taking care of all that. Businesses are now able to focus on their core business by outsourcing all the hassle of IT infrastructure. Some of the most important advantages of cloud computing are: cost efficiency, convenience and continuous availability, backup and recovery, cloud is environmentally friendly, scalability and performance, increased storage capacity, quick deployment and ease of integration.

There are three basic kinds of cloud service models. Each share similarities but have their own distinct differences as well. These service models are Infrastructure-as-a-Service, Software-as-a-Service and Platform-as-a-Service. It helps to think of these services in layers. Figure.2 depicts cloud service models.

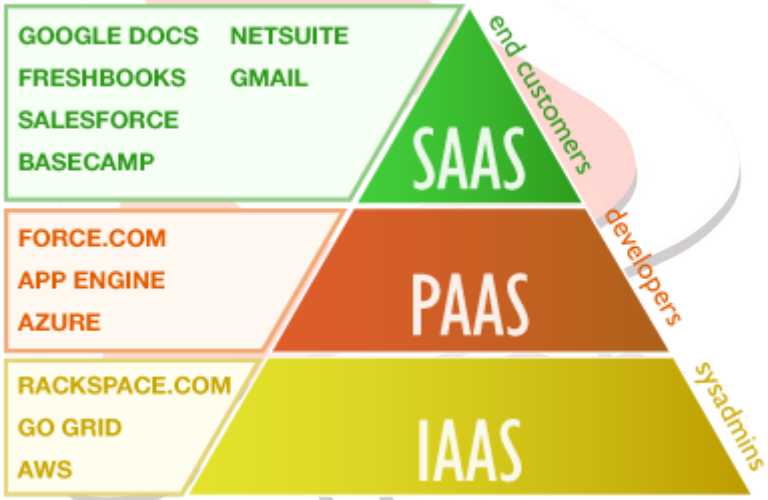

Figure.2

- **Infrastructure-as-a-Service (IaaS):**

  Infrastructure-as-a-Service is the first layer and foundation of cloud computing. Using this service model, you manage your applications, data, operating system, middleware and runtime. The service provider manages your virtualization, servers, networking and storage. This allows you to avoid expenditure on hardware and human capital; reduce your ROI risk and streamline and automate scaling. An example of a typical need for this model is someone who needs extra data space for processing power on occasion. Infrastructure-as-a-Service allows you to easily scale based on your needs and you only pay for the resources used.

- **Platform-as-a-Service (PaaS):**

  This cloud service model could be considered as the second layer. You manage your applications and data and the cloud vendor manages everything else. Benefits for using Platform-as-a-Service include streamlined version deployment and the ability to change or upgrade and minimize expenses. A business with limited resources interested in app testing or development might find Platform-as-a-Service beneficial to eliminate costs of upkeep for hardware. In this model, your business benefits because it is not necessary to hire people to maintain these systems.

- **Software-as-a-Service (SaaS):**

  This is the final layer of the cloud services model. This allows your business to run programs in the cloud where all portions are managed by the cloud vendor. Users will have assured compatibility and easier collaboration because all will be

using the same software. Your company won't need to pay extra licensing fees and you can easily add new users. As consumers we interact with Software-as-a-Service based applications everyday without even realizing it.

If you have a team that is able to maintain your hardware, but you want to make it easier to streamline your software programs for ease of use and compatibility, Software-as-a-Service will best suit your needs. Larger companies are a good example to use in this scenario. Teams of large people need to be able to work collaboratively in order to achieve your company's goals. By using Software-as-a-Service your team will be able to access the software from a variety of devices, in the office or on the go, which allows easier collaboration among your team.

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud. In a private cloud, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party. In a community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider. A hybrid cloud is a combination of different methods of resource pooling. Figure.3 represents types of clouds.

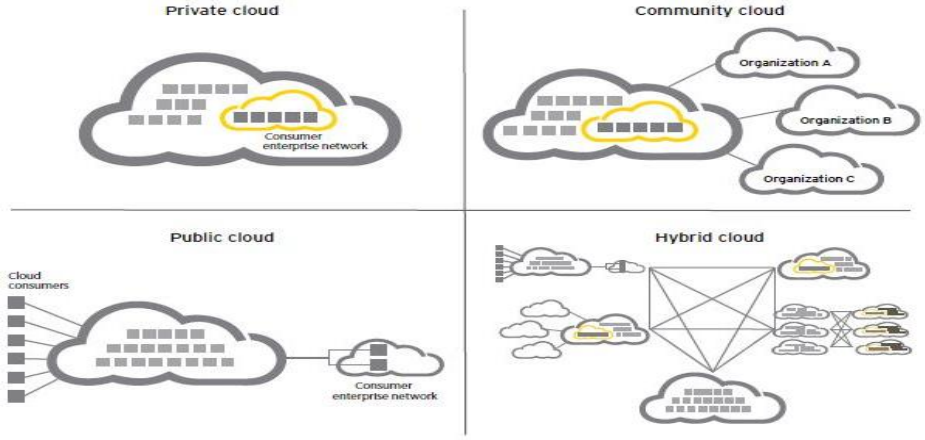

Figure.3

II. RELATED WORK

Several papers have been studied in the area of cloud computing security. Cong et al [3] proposes the system uses homomorphism token with distributed verification of erasure coded data. It effectively detects an unauthorized access in cloud environment.

Xian Liang [5] proposes a model to manage the virtual machine image in a cloud environment in secure manner. The advantage of this system is that the access permission is private so that untrusted parties cannot access the system. The main drawback is that the image filters cannot be accurate so that system does not eliminate the risk entirely.
Traynor. P [14] proposes data protection as services, which offer data security and privacy on cloud platform. These services can be provided using full disk encryption technique but it slow down data access time.

Farzad Sabahi [21] proposes the method to provide the security by implementing Hypervisor-based Technology to the data stored in third party area. But still there is a lack of security exists in cloud computing.

III. SECURITY ISSUES IN CLOUD COMPUTING

With the fast growing of cloud computing technology it introduces more vulnerability. So security is considered to be one of the most critical aspects in cloud computing environment due to the confidential and important information stored in the cloud. There are a number of vulnerabilities that should be considered by an organization when an organization is ready to handle their critical applications with cloud computing environment. These vulnerabilities are described as follows:

- **Virtual Machine Attack:**
  Virtualization is an important aspect of cloud computing where the software, operating system and all associated components are combined together such that it is independent of the hardware. To run client specific application each user has a virtual machine in virtualized environment of cloud. As there are multiple VMs that are running parallel in operating system of cloud provider. Therefore it is a tough task to manage the entire VMs. In this type of vulnerability it is tedious task to recognize where a particular target VM may reside. In this attack new VMs instance is created until one is placed in the target area.

- **Malware Injection Attack:**
  Cloud malware injection attack refers to a manipulated copy of the victim's service instance, uploaded by attacker to cloud, so that some service requests to the victim's service are processed within that malicious instance. An attacker

can get access to user data through this attack. The attacker actually exploits its privileged access capabilities in order to attack that service security domain. The incidents of this attack include credential information leakage, user private-data leakage and unauthorized access to cloud resources. The challenge does not only lie in the failure to detect the malware injection attack but also in the inability to determine the particular node on which the attacker has uploaded the malicious instance.

- **Insecure cryptographic storage:**

  In the cloud, the need to store sensitive information by the web application in the database is important. The information can be a credit card number, account details and username & passwords or any other private information. Therefore, the use of encryption is necessary. Amateur users usually make a mistake while using encryption. Failure to cipher critical data, insecure storage of keys, certificates and passwords, poor selection of encryption algorithms are a few of the major mistakes.

- **Session riding and Hijacking:**

  Session riding refers to the hackers sending commands to a web application on behalf of the targeted user by just sending that user an email or tricking the user into visiting a specially crafted website. Example of session riding includes deleting of user data, executing online transactions like orders, sending spam to an intranet system via internet. While session hijacking means using of a valid session key to gain unauthorized access of the information that is residing on a computer system that gives the chance to hackers to accomplish a wide variety of malicious activities.

- **Vendor lock-in:**

  Vendor lock-in is a situation in which a customer using a product or service cannot easily transit to a competitor's product or service. Vendor lock-in is usually the result of proprietary technologies that are incompatible with those of competitors. However, it can also be caused by inefficient processes or contract constraints, among other things.

- **Insecure APIs:**

  Cloud computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third-parties in order to enable their agency.

- **Denial of service attack:**

  The denial of service attacks mainly focus on web resources, those are provided by cloud service provider. Some of the security professionals suggested that cloud is vulnerable to denial of service attacks, because of its sharing of resources among their clients. The DOS attacks ensure more damage to the compromised resources in cloud environment. The cloud computing operating system poses the heavy workloads on distributed services, then the cloud try to provide more computing power to the resources about workloads. Thus, the server component boundaries are extended to maximum workload to process for no longer hold. By this way the cloud host is trying to work against intruder up to some extent even it supports the attackers by damaging services on resources. Due to this activity service availability decreases. As shown in Figure.4

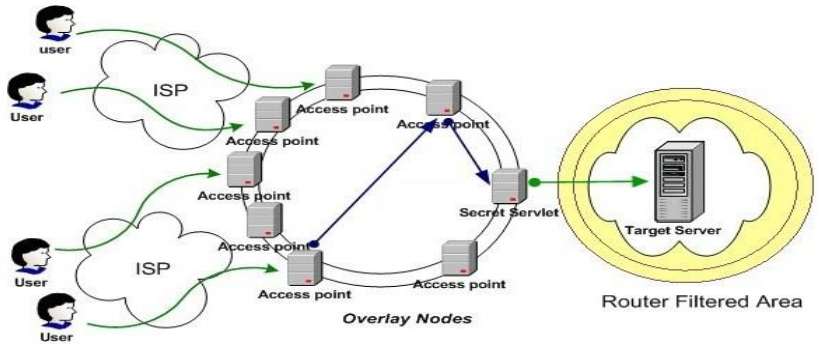

Figure.4

- **Data loss and leakage:**

  Data loss, which means a loss of data that occur on any device that stores data. It is a problem for anyone who uses a computer. Data loss happens when data may be physically or logically removed from the organization either intentionally or unintentionally. The data loss has become a biggest problem in organization today where the organizations are in responsibility to overcome this problem. Data Leakage is an incident when the confidentiality of information has been compromised. It refers to an unauthorized transmission of data from within an organization to an

external destination. The data that is leaked out can either be private in nature and are deemed confidential whereas Data Loss is loss of data due to deletion, system crash etc. Totally both the terms can be referred as data breach, it has been one of the biggest fears that organization face today.

IV. DATA SECURITY AND INTEGRITY IN CLOUD COMPUTING

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success. The world of computation has changed from centralized to distributed systems and now we are getting back to the virtual centralization. Location of data and processes makes the difference in the realm of computation. We have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So, logically speaking, the client has no control over it. The cloud computing uses the internet as the communication media. When we look at the security of data in the cloud computing, the vendor has to provide some assurance in service level agreements to convince the customer on security issues.

- **Privacy Enhanced Data Outsourcing in the Cloud:**

How to secure outsourcing data in cloud computing is a challenging problem, since a cloud environment cannot be considered to be trusted. The situation becomes even more challenging when outsourced data sources in a cloud environment are managed by multiple outsourcers, who hold different access rights. The data stored in a cloud database is considered as data outsourcing, since they are managed by an external party. For a consideration of security, the outsourced data are generally encrypted so that only authorized users can access them. Generally, these outsourced data consist of many data blocks. Data encryption before outsourcing is the simplest way to protect data privacy and combat unsolicited access in the cloud and beyond. But encryption also makes deploying traditional data utilization services such as plaintext keyword search over textual data or query over database a deceit task. At a high level, a searchable encryption scheme employs a pre built encrypted search index that lets users with appropriate tokens securely search over the encrypted data via keywords without first decrypting it.

- **Privacy-preserving access control for cloud computing:**

The problem of access control on outsourced data to "honest but curious" cloud servers has received considerable attention, especially in scenarios involving potentially huge sets of data files, where re-encryption and re-transmission by the data owner may not be acceptable. Data security, as it exists in applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users. Data confidential against cloud servers is hence frequently desired when users outsource data for storage in the cloud. In some practical application systems, data confidentiality is not only a security/privacy issue, but also of juristic concerns. As a significant research area for system protection, data access control have been developed to effectively implement fine-grained access control, which allows flexibility in specifying differential access rights of individual users. In access control architectures the data owner and cloud servers are very likely to be in two different domains. For the purpose of helping the data owner enjoy fine-grained access control of data stored on untrusted cloud servers, a feasible solution would be encrypting data through certain cryptographic primitive(s) and disclosing decryption keys only to authorized users. Unauthorized users, including cloud servers, are not able to decrypt since they do not have the data decryption keys.

- **Public remote integrity check for private data:**

Remote data integrity checking is a crucial technology in cloud computing. Recently many works focus on providing data dynamics and public verifiability to this type of protocols. Storing data in the cloud has become a trend. An increasing number of clients store their important data in remote servers in the cloud, without leaving a copy in their local computers. Sometimes the data stored in the cloud is so important that the clients must ensure it is not lost or corrupted. While it is easy to check data integrity after completely downloading the data to be checked, downloading large amounts of data just for checking data integrity is a waste of communication bandwidth. In remote data integrity checking protocols, the client can challenge the server about the integrity of a certain data file, and the server generates responses proving that it has access to the complete and uncorrupted data. The basic requirements are that the client does not need to access the complete original data file when performing the verification of data integrity and that the client should be able to verify integrity for an unlimited number of times.

- **Privacy enhanced keyword search in clouds:**

To ensure confidentiality, the sensitive data are usually encrypted prior to being outsourced. Nevertheless, effective data utilization remains a challenging task and there is a clear need for a secure and efficient searching mechanism over the encrypted data in the cloud, to increase the usability of the secure cloud environment. Unfortunately, existing works in the area of secure searching in the outsourcing scenario usually incur high computational complexity, which makes the approach impractical because some of the devices such as mobile are only equipped with limited computational power, the searching mechanism should be very efficient, and it should ideally avoid using the relatively expensive techniques. Keyword search is very simple, and it enables efficient multi-user keyword search over outsourced data files in the cloud environment.

V. CONCLUSION

Cloud computing offers some exciting opportunities for increased collaboration, working remotely and globally, and cost savings. While there are risks associated with moving to the cloud, the risks are no greater than when services are hosted internally. Cloud

computing by itself is in evolving stage and hence the security implications in it aren't complete. Achieving complete solution for legal issues is still a question. With this level of issues in cloud computing, decision to adopt cloud computing in an organization could be made only based on the benefits to risk ratio. The virtual environment of cloud computing users must transfer data throughout the cloud. Typically, cloud users know neither the exact location of their data. Consequently, several data security and integrity concerns have arisen, including access control, searchable encryption techniques, remote integrity checks etc. One possible method to enforce data access control without relying on cloud servers could be to encrypt data and disclose the corresponding decryption keys only to the privileged users, but that causes high performance costs.

REFERENCES

[1]. Kevin Hemalen, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham, The University of Texas at Dallas, USA, "Security Issues for cloud computing", April-June 2010, international Journal of Information Security and Privacy.

[2]. Ayesha Malik, Muhammed Mohsin Nazir,"Security Framework for Cloud computing environment: Review', *Journal of Emerging Trends in computing and information sciences*", Vol;3, No:3, March 2012, ISSN 2079-8407.

[3]. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International workshop on Quality of Service, 2009, IWQoS, Charleston, SC, USA, July 13-15, 2009, ISBN: 978-1-4244-3875-4, pp.1-9.

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

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

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

[7]. Sara Qaisar, Kausar Fiaz Khawaja, "Cloud Computing: Network/Security Threats and counter measures", Interdisciplinary Journal of Contemporary Research in Bus

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

[9]. 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.

[10]. Phaphoom.N, Wang. X, Abrahamson.P." Foundations and Technological Landscape of Cloud Computing" (ISRN Software Engineering Volume 2013 (2013), Article ID 782174, 31 pages)

[11]. D. Ramesh, A. Krishnan "An Analysis on Energy Efficient System Design in Grid Computing"(Second International Conference, CCSIT 2012, Bangalore, India, January 2-4, 2012.

[12]. Y. Song, H. Wang, Y. Li, B. Feng, Y. Sun, "Multi-Tiered On-Demand Resource Scheduling for VM-Based Data Center"(9th IEEE/ACM International Symposium on Cluster Computing and the Grid, China, pp: 148–155, 2009.)

[13]. A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2011.

[14]. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In Proc. of CCS'06, New York, NY, USA, 2010.

[15]. M. Chase. "Multi-authority attribute based encryption". In Proc. of TCC'07, Amsterdam, Netherlands, 2007.

[16]. L. Cheung and C. Newport. Provably Secure Ciphertext Policy ABE. In Proc. of CCS'07, New York, NY, USA, 2007.

[17]. V. Goyal, A. Jain, O. Pandey and A. Sahai, "Bounded Ciphertext-Policy Attribute based Encryption", In Proc. of ICALP'08, Reykjavik, Iceland, 2013

[18]. Jin Li, Qian Wang, Cong Wang, and Kui Ren, "Enhancing Attribute-based Encryption with Attribute Hierarchy," In Proc. of ChinaCom'09, Xi'an, China, 2009.

[19]. "Amazon Web Services: Overview of Security Processes", Whitepaper, May, 2011.

[20]. Justin Clarke; SQL Injection Attacks and Defense; Syngress 2009; ISBN-13: 978-159749424.

[21]. Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", Int. Journal of Machine Learning and Computing, pp. 39-45, vol. 2, no. 1, February, 2012.

[22]. Larry Dignan (Editor in Chief- ZDNet), "Epsilon Data Breach: What's the value of an email address", IT Security Blogs, Tech Republic, April 5, 2011.

[23]. Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research", IEEE Internet Computing Journal, vol. 13, issue. 5, pp. 10-13, September 2009.

[24]. Julisch, K., & Hall, M., "Security and control in the cloud", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2012.

[25]. Sangeeta Sen, Rituparna Chaki, "Handling Write Lock Assignment in Cloud Computing Environment", Communications in Computer and Information Science, vol. 245, issue. 7, pp. 221-230, 2011.

[26]. Mervat Adib Bamiah, sarfraz Nawaz Brohi, "Seven Deadly Threats and Vulnerabilities in Cloud Computing" *International Journal of Advanced Engineering Sciences and Technologies*, Vol No. 9, Issue No. 1, pp: 087 – 090