International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 10 (2018) pp. 8390-8406

A Survey on Data Storage Security Issues in Cloud Computing

Mrinal Kanti Sarkar
Department of Computer Science & Engineering
University of Engineering & Management, Jaipur, India.

Sanjay Kumar
School of Computer Science & Engineering
Jaipur National University, Jaipur, India.

Abstract

Cloud computing provide on demand computational infrastructure to the users which has the latent to reduce the huge cost to assemble IT based services. It can offer ubiquitous, expedient data storage space. One of the main significant issue of cloud computing is that the entire data are stored in different location of the world using a set of interconnected resource pools and an authorized user can access this data through virtual machines. Most of the today's internet companies have built immense data centers and day by day it is growing incredibly. For this reason we are getting various types of cloud flavor in terms of excellent applications or services. But it has several dark sides and insecurity creates major problem for cloud users. Since the resource pools are situated over various corners of the world, the privacy and security of data is highly challenging. Due to new dimension of cloud computing, the security problem enters into the problem scope related flexibility, multi-tenancy, layer dependency over its architecture. There are several types of security issues that need to be address in cloud computing. The main aim of this paper is to focus on various security issues of cloud computing and analyze the different unsolved security problem that threatening the different organization to adopt this technology.

Keywords: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Security, Privacy, Integrity, Virtualization.

INTRODUCTION

Cloud Computing (CC) is a future generation technology for IT enterprise. It work from the remote locations without need of human intervention. It is not essential for any user to know how their computers, their software or their network is working as per the user need. In such model, user only uses services as per their requirements without having the knowledge of location where these services are stored. Even users do not require owning the infrastructure for the purpose of computing for the different services. In fact it can be accessed from any computer from any part of the world. It can arrange resources dynamically to allocate or reallocate to user and can monitor its performance continuously [1].

Though there are several services which cloud provides to the client companies or any other users. All users can get huge amount of storage capacity, but most of the client are not geared up to implement cloud computing technology due to the limitation of security control strategy, limitation in protection data which leads to dispute in cloud computing. The cloud computing vendors, like Amazon Simple Storage Services (S3) and Amazon Elastic Compute Cloud (EC2) [2] are well known example. Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It also permit developer to right of entry the extremely scalable, dependable, safe, speedy, low-cost infrastructure. From the belief of data protection which has been an important facet of worth of services, cloud computing necessarily poses new demanding safety threats for number of reasons. Cryptographic techniques to ensure data security in cloud computing are not gladly acceptable as the user' can lose their control over data. So, it requires a data authentication strategy but without unambiguous knowledge of the complete data, it is very inflexible to verify the accurate data. Considering a range of data for each user, insist of the long term incessant assurances of their data safety, the problem of verify the accuracy of data storage in the cloud becomes more challenging [3]. Secondly, it is not just an intermediary data storehouse because all the data are stored in the cloud and may be regularly modernized by the user, such as inclusion, removal, alteration, appending, recovering, etc. So, for this dynamic operation, it need to more advanced technology to prevent data loss from the cloud storage. Every user' data is stored in numerous physical locations haphazardly. Therefore scattered protocols for storage correctness assertion will be most significance to achieve a healthy and protected cloud data storage system is required in the real word.

As users are storing their data and running their software on somebody's CPU with facilitate of someone else's hard disk, it will countenance malevolent security issue such as phishing, loss of data and collection of machines that are running remotely known as botnet. Moreover, the multi-tenancy and shared computing resources have introduced usual types of security challenges that need fresh techniques to deal with it. For example, hackers may use cloud to systematize botnet because cloud often offer more consistent infrastructure at a comparatively low price for them to initiate an attack [4].

Rest of the paper is organized in the following way. After giving the brief introduction of cloud architecture in Section II, we present the different data storage issues in Section-III.

In Section-IV we have discuss the different types of attacks with their possible solution by ending the conclusion and future work in Section-V.

ARCHITECTURE OF CLOUD COMPUTING

Cloud computing can be mostly classify in two categories, deployment models and service delivery models [1]. The deployment model is: 1) Private cloud: a cloud platform is

committed for particular organizations, 2) Public cloud: a cloud platform which is accessible for all users and can use all available infrastructures, 3) Hybrid cloud: a private cloud that can enlarge to use resources in public clouds. Public clouds are the maximum vulnerable deployment model because it is accessible for public users to host their services who may be malicious users and 4) Community Cloud: This cloud infrastructure can be used by an explicit community of consumer from the organization if they have some shared concern. The NIST definition of Cloud Computing is shown in Figure-1 which has different promising implementations that move up the complexity to develop security model.

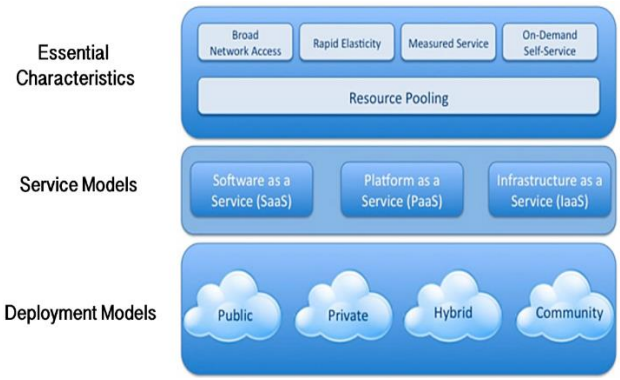

Figure-1. The NIST Definition of Cloud Computing Source: http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

The service delivery model is organized into three layers, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)-generally known as SPI model.

Infrastructure as a Service (IaaS) is considered as the lowest layer that provide infrastructure as a service. It is very much popular and developed for market segment of cloud computing. The available option within the IaaS varies from single server to entire infrastructures including network devices, database, web servers etc. It provides hardware resources for executing services to the user by using virtualization technology. The cloud user has the facility for processing, storage, networks etc. A governance model is needed to control the creation and usage of virtual machines.

Platform as a Service (PaaS) is the middle layer which provides platform oriented services, besides providing the environment for software execution. PaaS solution provides a development and deployment platform for running application in the cloud. Its implementation offer application with a run time environment and manage the underline infrastructure without exposing the services. It automate the process of deploying application such as infrastructure, configure application component, supporting technology like balance the databases, policy based system which is set by the user.

Software as a Service (SaaS) is the topmost layer which has a complete application and provides services on demand. It is a software delivery model which provide to access application through the internet as a Web-based service to user without installing the application on the user's own computers. Each service delivery model has different possible implementations, which complicates the development of standard security model for each service delivery model.

The requirement characterizes Software-as-a Service as a "one to-many" software delivery model where applications shared across the multiple users. SaaS applications comprises of social networking applications. The basic features of networking are to allow inculpating and extend their capabilities by integrating third party application. It is an important role of SsaS solution to provide an environment to share information with others. The vendor such as SalesForce.com, Google Mail, Google Docs, and so forth is providing SaaS. Each service delivery model has different possible implementations, which complicates the development of standard security model for each service delivery model.

It is understandable that the security issue is playing most central role in hindering cloud computing acceptance. It is very difficult to store your data on someone else's hard disk, running your software on using someone else's CPU which is daunting to many. The very popular security issues such as data loss, phishing etc pose serious threats to organization's data and software. The characteristics of multi-tenancy and pooled computing resources of cloud computing has introduced new security challenges which need a novel techniques to protect all benefits of cloud computing.

There are some early computing paradigms like Global Computing, Grid Computing, On Demand Service Provision, User Centric Interface, Autonomous System [5] etc. Though the following other computing technology which contribute to the cloud computing.

- *Web Service and SOA:* Web services are software systems which has been designed to support interoperable machine-to-machine interaction over a network. The interoperability can began through a set of XML-based open standard application, such as WSDL, SOAP, and UDD where a service-oriented architecture is essentially a collection of services [5]. These services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some other activity like connecting services to each other whenever is needed.
- *Web 2.0 and mash-up:* A mash-up is a Web page or application that incorporates complementary components from two or more sources. Web 2.0 known as a technology to enable us to build web pages and there is no limit for a user to viewing only as well as it permits the users to make dynamic updates. It allows the usage of World Wide Web technology towards a more inventive and a collective platform [6].
- *Application Programming Interface:* (API) is a collection of protocol, subroutine and outfits to the software applications. The API stipulates that how a software modules should in cooperate and APIs are used in programming graphical user interface section. Without API's it is hard to believe the

existence of cloud computing. The complete groups of cloud services depend on API's which permits to deploy and configure through them. Application programming interfaces help developer to use certain technologies to develop several applications. A single API can have multiple implementations in the form of different libraries that share the same programming interface by abstracting the underlying implementation and only exposing objects or actions.

- *Virtualization:* The Virtualization lead to the evaluation of cloud computing. The term virtualization means to create a virtual adaptation of a device or resource, such as a server, storage space device, network or even an operating system where the structure divide the resource into one or more effecting environments. Even sometime it is a simple hard drive partition which considered as virtualizations because we take one drive and partition into two separate hard drives [7]. It has been categorized as server virtualization, storage virtualization and network virtualization.

SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing has different types of properties which make it very valuable. But, many of those properties are creating security as a singular concern. Though several tools and techniques are available which can be used to keep your data safe, but it is very hard to keep up the reliability of your system as you are sharing your data with others and most of the time it is outsourcing from others. The cloud architecture model has different types of loopholes and this architecture made cloud computing into various security and privacy threats [8].

Security Issues in the Cloud Service Delivery Models

There are different types of implementation of cloud service delivery model and this implementation creates to develop the standard security model for each service delivery model. The following are some security issues in the cloud service delivery model.

IaaS Security Issues

The available option within the IaaS varies from single server to entire infrastructures including network devices, database, web servers etc. It provides hardware resources for executing services to the user by using virtualization technology but IaaS will face the following problem.

- *VM Security*- Virtual machine is a logical machine in which applications and guest operating systems run. By design, all virtual machines are secluded from each other and seclusion enables multiple virtual machines to run firmly when it is sharing hardware. It ensures capability to access hardware and their uninterrupted performance simultaneously. VM operating systems and its workloads are common security threats that affect conventional physical servers, such as malware and virus using traditional or cloud-oriented security solutions. Cloud consumers are responsible for VM security. They can use their own security mechanism based on their need to overcome the expected risk level and their own security management process [9].
- *Securing VM Images repository*- It has been observed the VMs are often under risk even when they are offline unlike the physical servers. VM images can be stolen by injecting malicious codes even it can be hampered by the VM file itself. So, cloud provider is responsible to secure VM images repository. It may be happen that VM templates may retain the original owner information and this information template may be used by a new consumer.
- *Virtual Network Security*- network infrastructure is shared among different tenants in the physical networks or within the same server (using virtual Switch). Network-based VM attacks may be arise in DHCP, DNS servers, IP protocol vulnerabilities, or even the in VSwitch software.
- *Securing VM boundaries*- There is some virtual restrictions in VMs compare to physical server ones and it co-exist on the equivalent physical server that share the same CPU, Memory, I/O, NIC, and others as there is no physical isolation among VM resources. So, cloud provider has the responsibility to secure VM boundaries.
- *Hypervisor security*- The mapping between physical resource and virtualized resource can be accomplished by a virtualizer, known as hypervisor. Access to physical server by virtual machine can be achieved by hypervisor controller. Operations of virtual machine are not in an encrypted form and that is why every hypervisor takes a major role to provide the security of the virtual machines. Compromised hypervisor may break the security of VMs. On the other hand cloud service providers are the responsible entity to provide the security of hypervisor. CSP provides this type security in Virtualization software like VMware etc.

PaaS Security Issues

Out of several clouds computing services, platform as a service allows the user to customize the applications in the form of development, execution and management. This platform as a service (PaaS) follows service oriented architecture. So the security issue of PaaS is all lies on SOA security. SOA security includes multiple perspectives of security issues comprising access control, privacy and service stability while shielding both the cloud service provider and the cloud user. All most, all kind of security attacks preferably Denial of service of attacks and man in the middle attack may disrupt the service provided by PaaS.

API Security- Application Programming Interface (API) offered by Platform as a service provides various functions related to business and management. These PaaS level APIs should maintain security mechanism and standards like OAuth [10] in order to prevent vulnerabilities. These APIs should be separated from each other in device memory for security purpose. This API level security issues are controlled by cloud service provider.

SaaS Security Issues

Software as a Service (SaaS) is the topmost layer which has a complete application and provide services on demand. It is a software delivery model which provide to access application through the internet as a Web-based service to user without installing the application on the user's own computers. Each service delivery model has different possible implementations, which complicates the development of standard security model for each service delivery model. The SaaS model facing different types of issues as follows [11]:

- Data security: A malicious users can take advantage of weakness in the data security model to expand unauthorized access to data.
- Network security: A secured network will be needed to flow all the data over the network in order to prevent outflow of responsive data.
- Data Locality: A secure SaaS model will be capable of providing reliability to customer on the location of the data.
- Data Integrity: The lack of veracity controls at the data level could result in intense problems. Architect and developers need to approach this problem seriously making sure that there will be no compromise with database integrity when user is moving to cloud computing.
- Data segregation: A nasty user can practice application liabilities to hand skills parameters that avoid security checks and access responsive data of other renter. SaaS model must need a boundary to secure each user data. This limit must be guaranteed to the physical level as well as with the application level. The service should be clever enough to isolate the data from different user.
- Data Access: The security policies must be considered by cloud to avoid intrusion of data by unauthorized user.
- Authentication and Authorization: Many times a user credential are stored in the SaaS providers database, so need a proper mechanism to store that credential so that authentication and authorization credential will be safe.
- Data Confidentiality: The entire contents of user's storage devices may be stored with a single cloud provider or with many cloud providers. So when these storage devices are shared the information in the cloud, confidentiality or privacy question arises.
- Availability: It needs to ensure that the user data will be available around the clock so that user can access their data any time.
- Backup: As all the user data are very sensitive, so need a backup mechanism so that user data will be recovers any time due to any unwanted incident.
- Identity management and sign-on process: Identity management is a broad area that deals with identifying the each user and gives the permission to control the resource by entering into the system by providing the correct credentials.
- Data breaches: Several user and organization store the data in same location in a cloud environment. So, the data of all users will be breached by the insider. Though insider don have the permission to access the data directly, but they have different way to access the database.
- Web application vulnerability scanning- web based applications need to be validated and should be well scanned prior to host on the cloud infrastructure. Scanning up on susceptibilities can be achieved by various application oriented scanning techniques [12]. These scanning techniques must be updated with latest features in order to provide proactive protection against most of the recent vulnerabilities and intrusions specified by NVD and CWE [13]. Application and proxy firewall should be configured and properly distributed in appropriate place so that it can monitor incoming and outgoing responses/requests in a filtered manner otherwise malicious scripting or malicious packet injection methods may hammers overall reliability of web application hosted on cloud infrastructure.
- Web application security miss-configuration and breaking- web application security in SaaS is very much essential. If there is any weakness or problems in configuration then total security protection will be broken. In case of multi-tenant system, each tenant has their own security configurations. Now if the security configuration is not same for each tenant then a security gap will be arise. To address the security gap problem like miss-configuration, there must be some new security protocol provided by cloud providers in consistent manner.

Cloud Management Security Issues

Cloud Management Security issues include a separate layer called Cloud Management Layer (CML) to deal with various components associated with cloud management. This CML acts like a kernel in operating system to manage all the components. This layer is very much vulnerable to attack and as a result whole cloud platform may be compromised any time, any moment. So security mechanism should be implemented in each and every components of CML. More over CML offers same API like PaaS, so PaaS level security is also applicable for CML.

Cloud Access Methods Security Issues

Cloud computing architecture is build based on sharing resources over the internet. Cloud resources can be accessed in the following way:

- Through Web Browser like Mozilla, Google Chrome, Internet Explorer etc.
- Internet communication protocol like IP, REST or some remote client-server application protocol.
- Remote connections, VPN, TELNET, SSH or FTP.

Each of the above techniques must deal with security and privacy issue.

Security Issues in the Cloud Deployment Models

Cloud Deployment Models can be classified as:

- Public cloud
- Private Cloud
- Hybrid Cloud

Each and every model has its own service area. Every model is comparable with each other on the basis of services which it is offering. Not only services but also security issues are different for different models. Various security issues of different cloud models are discussed below:

Public Cloud Security Issues

In public cloud, the customers share same cloud platform and SOA security is offered by the cloud service provider itself. Some important security issues in a public cloud are as follows:

- Some common security parameter like confidentiality, integrity and availability are essential to keep data safe for the entire period of life. The public cloud life cycle consists of following stages: creation, data sharing, data archiving, and data processing. During the period of public cloud life cycle, the data must be protected from any kind of intruder or malicious entity. In case of public cloud the security issues are not controlled and that is why public cloud life cycle becomes more vulnerable for any kind of attack [14].
- In public cloud, the similar kind of platform is distributed between various customers and there is high chance of illegal sharing of data between these customers. Now a day's most of the cloud service provider provide multitenant environment and that's why proper validation and authentication should be done prior to choose any cloud service provider [14, 15].
- If a Cloud Service Provider hires third party vendor to provide its cloud services then the service level agreement, terms and conditions and other protocols between them must be checked precisely so that the service reliability and integrity is preserved.
- Proper Service Level Agreements featuring the security requirements like standard encryption technique, when the technique is placed over the internet and what kind of penalties in case the service provider fails. Even the data is stored outside of the client organization in a public cloud, but still there is a chance of intruder involvement originating from cloud service provider ends. Storing the data to a cloud environment increases the provision of insiders to the service provider's controller and sub controllers [16]. In paper [17] policy on access control has been discussed to prevent the internal intruders both from cloud users and cloud service providers. The policy is implemented at node level as well as at data center level. This policy is built upon the following stages
  - Specification or definition of the policy
  - Execution or propagation of the policy in all levels
  - The performance measurement of the policy

Private Cloud Security Issues

Private cloud model allows the cloud user to have full regulation over the cloud system and offers the freedom to the cloud user to establish any state of the art network frontier security drill. Even the private cloud is much secured than public cloud but still there is some risk that has to be addressed in private cloud.

- Virtualization methodologies are pretty common in case of private clouds. In such a situation, there is a chance of hypervisor to become compromised by some malicious agent. So in this case malicious agents or threats must be addresses carefully. It is seen that virtual machine can create network among them and communicate with each other. But if the virtual machine is not the part of that VM network but still participate in the communication then it creates risk for the virtual machine. All cooperated VMs can join to communicate to each other but it needs strong verification techniques like IP level Security etc should be implemented [18].
- The operating which is being host must be free from any kind of virus, malware, threat or worms and monitoring system should maintain minimum standard to avoid such kind of problems [19]. On the other hand virtual machines must communicate with dedicated physical interface.
- In private cloud, customer gets privilege to manage the parts of the cloud platform. Not only to manage but also clouds customers' gets benefit in order to access the cloud infrastructure. And this opportunity is delivered through a web application interface (Web API) or via HTTP connections. Three options are there to implement web application interface as follows:
  - Writing a complete application stack
  - By using standard application stack
  - Using object oriented programming languages like JAVA, Python etc.

Through screening process it is observed that the Eucalyptus web interface has a bug. It allows cloud user to execute inner port scanning or HTTP requests via the controlling node which users should not be permitted to do so. In case of nutshell, interfaces must be accurately implemented and updated version of web application security methods must be installed to defend the various HTTP requests being accomplished [20].

- Security policies are the blueprint for a security policy. However policies do not talk about how to develop security technique. But it talks about what restriction should be put on those security controls. People rather talk about standard of the security than the guidelines or policies of the security technique. But one thing always need to remember is that the security blueprint or policies are equally important as the standard of security software [19].

Community Cloud Security Issues

Community cloud actually lies in the middle of public and private clouds with respect to the concern group of users. It is very much closer to the private cloud, but there is some dis-similarity as follows:

- Two or more organization exclusively infrastructure and computational resources.
- All organizations have common privacy, security, and regulatory concerns, rather than a single organization [21].

The community cloud aims to conglomerate the followings:

- Distributed supply endowment from grid computing,
- Distributed regulation from digital ecosystems
- Distributed sustainability from green computing
- Achieving sustainability with the help of cloud computing, during self-management from autonomic computing.
- Replacement of retailer clouds by influencing the unutilized resources of user machines possibly fulfilling the roles of consumer, producer, and most importantly coordinator [22].

Hybrid Cloud Security Issues

The hybrid cloud model is an amalgamation of both public and private cloud. Now the security issues of hybrid cloud is similar to private and public cloud. If we discuss security issues of private and public cloud then it will cover the entire hybrid cloud security issues. Public cloud is much more intruder prone in compare to private cloud due to its shared or openness characteristics. But sometimes private cloud also suffers from some security loopholes. Those loopholes must be addressed properly on time in order to avoid any kind of security attack. Many cloud based security issues have discusses earlier but another most popular security mechanism called trust or reputation based security model is remain untouched. This trust base model includes some social security like total cooperation, coordination, honesty etc. [23]. There are many problems like multiple stakeholder problems, open space security problem and data handling problem can be addressed by the trust based cloud security model or security aware cloud.

Threat to Security in Cloud Computing

The main important tasks of cloud are to offer various services in terms of processed data to the end users. Many end users keep their data in cloud data storage and cloud providers provide the security on those data. Now if the security policy is not standard then the third party intruder or attacker can easily get the data of end users. In that case those particular cloud providers are not trustworthy and people will go for other cloud service providers which can provide better security services [24]. If there is any security issues in any mission critical system there must a smell of threat. Various cloud service delivery specific security threats has been discussed earlier in various paper. Proper identification and the classification of security threat is important prior to implement the security techniques and that can be achieved by rigorous survey on threat. Privacy and Security at different cloud layers such as application layer, Host layer and Network layer is compulsory to keep the cloud up and running uninterruptedly and this has been described in paper [25] for Amazon EC2 cloud. Various types of security holes may generate with the security issues of different layer mentioned in previous section. The security holes can be categorized as follows:

- Basic Security
- Network Level Security
- Application Level Security

Basic Security

Some robust technologies are used to enable Software as a Service (SaaS) that offers users to accomplish the tasks like installation, configuration and maintenance of software without any hassle. Web 2.0 is one of the rapid growing technologies that offer the users to customize the software by enabling SaaS [26, 27].

- *SQL injection attacks*: In case of SQL injection attacks some malicious code is injected into a Structure Query Language. By this process, third party malicious users easily get control over the database [28]. As a result of SQL injection attacks web server cannot distinguish between actual user's input and malicious user's input and hence shares the storage control to malicious user thinking that it's an original user. There are different types of techniques to prevent SQL injection attack. One of the proxy based technique is discussed in the paper [29] that vigorously distinguishes and excerpts users' inputs for mistrusted SQL control measures.
- *Cross Site Scripting attacks:* It injects mischievous scripts into web based contents. Now a days, it is much popular after Web 2.0. methods which are used to inject malicious code into web based content as follows:
  - Stored Cross Site Scripting
  - Reflected Cross Site Scripting
- *Stored Cross Site Scripting*: In this scripting malicious code stored into the web based content permanently. The attack is invoked when users request for dynamic content of a particular website in which user is logged in [30].
- *Reflected Cross Site Scripting:* Unlike Stored Cross Site Scripting, this reflected cross site scripting deals with the malicious code which is stored into the web based content temporarily rather than permanently. The effect of this attack is reflect immediate to the user [30]. Static or dynamic website categorized on the basis of the service that the website provides. A Static websites do not suffer from the security threats whereas the dynamic websites do because of their dynamism. Dynamic websites are very much prone to Cross Site Scripting attack. Many times it is observed that if the users click on any hyperlink, dynamic image or video then immediately Cross Site Scripting attack starts to perform. Few popular methods have been proposed in the paper [31] to deal with Cross Site Scripting attack like Web Application Vulnerability Detection Technology, Active Content Filtering and Content Based Data Leakage Prevention Technology. These technologies are very much efficient to detect the security holes and solve them. To reduce the dependency on web browsers in order to detect un-trusted

content over the internet, a blueprint based approach has been proposed in [32].

- *Man in the Middle attacks (MITM):* Man-in-the-Middle attack is nothing but the monitoring, capturing, and controlling of communication visibly by third party agent. In this case attacker can change the path of data exchange. When computers are communicating at data link or physical layer, the computers might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are basically like someone assuming somebody's identity in order to read somebody's message. This Man-in-the-Middle attack is associated with SaaS. The attack is skilled enough to damage the Software services as an application-layer attack. Tools like Dsniff, Cain, Ettercap, Wsniff, Airjack etc. have been developed to protect from Man –in-the-middle attack. [33].

Network Level Security

We can classify a network on the basis of service and scalability into following ways:

- Shared and non-shared network Ex: Shared Bus network or Mesh network.
- Public or Private network (Ex. Public and private cloud)
- Small area or large area networks like LAN, MAN or WAN respectively.

Now each and every type of networks deals with their own security measures. In some cases nature of the risk and threats are same for different types of network and sometime it may differs. As an example, security threat is more in case of public cloud and less in case of private cloud. So, private cloud is more protected than public cloud. Data confidentiality and Integrity needs to be ensured in case of public cloud architecture. Security attacks associated with public cloud are [34]:

- DNS attacks
- Sniffer attacks
- Issue of reused IP address
- Denial of Service (DoS)
- Distributed Denial of Service attacks (DDoS)
- BGP Prefix Hijacking

- *DNS Attacks:* Domain Name Server (DNS) is used to translate IP address into domain name as an example www.google.com, amazon.com etc. It is easier to remember domain name than to remember IP address. There is a possibility of security risk when cloud user looking for exact DNS server but somehow redirect to malicious cloud server. But we can reduce this kind of risk using Domain Name System Security Extensions (DNSSEC). However DNSSEC used as a DNS security measures but all the security risk related to DNS cannot be overcome [35].

- *Sniffer Attacks:* In case of Sniffer attacks, unencrypted packets transferring between sender and receiver get captured and valuable information can be retrieve easily by the sniffer attacker. Sniffer attacks starts from network interface card by keeping it in promiscuous mode and in promiscuous mode attacker can track all data, traversing on the same network. To detect such type of attack Address Resolution Protocol and Round Trip Time based mechanism is very useful and it is discussed in the paper [36].

- Reused IP Addresses: IP address can be reused using dynamic distribution of IP address. When a user change his or her network then the used IP address of previous network can be reassigned to another new user. Now new user can use the IP address used some other person and accomplish his or her task. In this case security risk may arise for the new user for a certain time as the change of the IP address in DNS and to clear the address from DNS caches [37].

- Denial of Service Attacks: A denial-of-service attack (DoS attack) is a an attempt to make the services like machine or network resources assigned to the authorized users unavailable to its intended users by momentarily or indeterminately disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. The server which providing the service is drowned by a large number of entreaties and hence it will fail to meet authorized requirements. DoS attack growths bandwidth consumption which makes certain parts of the clouds inaccessible to the users. The most popular method to overcome this is Intrusion Detection System (IDS) [38]. A method called as defense federation [39] is used to protect such types of attacks where each cloud is loaded with separate IDS. Based the information exchange, the different intrusion detection systems is working. In case a precise cloud is under attack, the co-operative IDS warn the full system. All the on trustworthiness decision will be taken by voting but without hampered the overall system performance.

- Distributed Denial of Service Attacks: Distributed Denial of Service (DDoS) can be termed as more advanced version of DDoS in terms of refusing the exclusive services executing on a server by spreading the destination sever with huge number of information such that the focused server is unable to handle it. In DDoS the attack is transmitted from different rapid changing networks which have already been biased unlike the DoS attack. The intruders have the potential to manage the flow of data packets by entertaining some information available on time. So, information which is available for the use of public is clearly under the control of the attacker [40]. The DDoS attack is being executed by three operational units: master, slave and victim. Master unit is the initiator behind all these attacks where slave act as a launch pad for the master to causing DDoS. It offers the stage to the Master unit to introduce the attack on the Victim device. For this reason it is also known as co-ordinate attack. Normally a DDoS attack is functional in two phases, the first phase is intrusion phase where the Master attempts to compromise ignored machines to provide support in flooding the more important one. The second phase is installing the DDoS tools

and hitting the victim server. Hence, a DDoS attack makes the service unreachable to the valid user like DoS attack but the way it launched is completely different from DDoS. Basically the schemes used to guard against DDoS attack involve rapid modification of the underlying network. Modifications in underlying network becomes worthy for the users. A swarm based scheme has been proposed to provide protection against the DDoS attack [40]. The swarm based logic offers an apparent transport layer, via which the well-known protocols such as HTTP, SMTP, etc. can bypass smoothly.

- *BGP Prefix Hijacking:* It is kind of network attack in which a false broadcasting related to the IP addresses of an Autonomous System (AS) is done. As a result fraudulent nodes get access to the undetectable IP addresses. An autonomous system can broadcast message which contain IP address to all its adjacent. Border Gateway Protocol (BGP) is used as a communicator between two ASs. Sometimes a faulty AS may broadcast false information about the IPs associated with it. As a result the original message gets diverted to some other IP address and data is leaked or reached to some other unwanted destination. A security for autonomous systems has been explained in [41].

Application Level Security

On the basis of the usage of software and hardware resources the application level security is provided. The intruders are not able to get the control of the applications and make required changes to their format due to application level security. Attacker always behaves like a trusted user in front of the system and gradually damaged the systems. It is necessary to install higher level of security software to reduce the risks [42]. Attackers are dynamic and adaptable to the security standard that's why in case of application level security closed systems are observed to be slower than open systems.

It is noticed so far that however a particular website is safe and secured at the network level with powerful security measures but there may be a chance of security gap at the application level. Application level is facing the threats like CAPTCHA Breaking, SQL injection attacks, XSS attacks, hidden field manipulation, Cookie Poisoning, Backdoor and Debug Options, DoS attacks, etc. due to illegal practice with applications.

- Security concerns with the hypervisor: Cloud Computing reposes mainly on the concept of virtualization. Virtual machine manager (VMM) which known as a Hypervisor. It is defined as a controller that permits several operating systems to be run on a system concurrently. It distributes resources to every operating system such that they do not impede with each other. Many operating systems are executing on a single hard disk and it increasing the security issues that need to be considered as it is not possible to monitor and maintain all the system simultaneously. Sometimes, there is a change that a guest system attempts to run a malevolent code on the host system and try to take control of the system or bring the system down and block all the access to other guest operating systems [43]. It is a very tough job to share the same hardware devices among many users as a malevolent can cause threats to the others using the same infrastructure. Security is a big deal with respect to hypervisor as all systems are controlled by it. If an unauthorized user is able to get control over the hypervisor, it can alter the resource to any of the guest operating systems and may get all control over all the data and can pass through the hypervisor. There are different types of attacks which have been launched to target different components of the hypervisor [44].
- Cookie Poisoning: All cookies stored the identity of user's with its credentials. If, it will accessible to the malicious user, the information of it can be copied to impersonate an unauthorized user. An unauthorized can change or modify the contents of cookie to a web-page or an application. This can be escaped either by performing consistently cookie cleanup or instigating an encryption scheme on the cookie data [45].
- Hidden Field Manipulation: When a user is accessing a web page, which has some field that is hidden from the user and this page contains some related information which is basically used by developers. These fields are highly disposed to attacks by an unauthorized user and it can be modified effortlessly and posted on the web-page.
- Backdoor and Debug Options: At the time of publishing a website, all developer common practice is to enable the debug option which permits to implemented on the website by changing the developmental code. As these debug options simplify back-end entry to the developers, and sometimes it may happen that these debug options are left enabled to unnoticed, this may offer cool entry to a hacker into the web-site that make changes at the web-site level [40] by a unauthorized user.
- CAPTCHA Breaking: CAPTCHAs had come in the market in order to protect the usage of internet resources by bots or computers. They are rapidly used to provide safe guard from spam and overexploitation of network resources by bots. CAPTCHA is also used to prevent even multiple web-site registrations, dictionary attacks etc. But recently, it is observed that the spammers especially from Hotmail and G-mail service providers are able to break the CAPTCHA [45]. These providers use audio system capable of reading the CAPTCHA characters for the visually compromised users and also use speech to text conversion software to overthrow the test. It was observed that the net users are offered some form of motivation towards solving these CAPTCHA's using automated systems and thus CAPTCHA Breaking takes place. Many companies like Facebook, Google adopted multiple authentication techniques to fight against CAPTCHA breaking.
- Google Hacking: Nowadays Google is the last and one of the best option to find details of anything over the internet. In case of Google hacking, hackers always intuitively try to find out the security holes by probing out on Google about the system they wish to hack. After gathering the required information, hackers carry out the hacking on the targeted system based on the loophole where hacker wishes to hack. Then hackers examine all the probable systems with such hole and catch those using the loopholes they wish to hack upon. Recently, it has been observed that various Gmail

users' account hacked by a group of hackers [46]. These threats should be monitored at the different levels of service delivery models in cloud like Infrastructure as a Service, Platform as a Service and Software as a Service. In case of an Infrastructure as a service delivery model, cloud providers are not aware with the security rules imposed by the user and the application's management. As all applications of user are executing cloud provider's server where it is controlled by them, so it needs to be secure the application. The following points must be taken care of while designing the application: Standard security measures must be applied to protect against the common susceptibilities associated with the web. Without testing properly the custom application of authorization and authentication schemes should not be employed. In case of a sudden attack, protection should be applied in order to skip the issues with data recovery. Various security challenges for Infrastructure as a service Cloud Computing and multi levels of security as functional in Amazon Elastic cloud computing have been discussed in [47]. It deals with identity management, service access management and multifactor authentication techniques in Amazon Web Service (AWS) cloud. Platform as a service providers are liable for implementing and maintaining the security of the cloud platform and for this purpose an application is built upon.

- Dictionary Attacks: In cloud computing environment, data security may be compromised by some intruders like dictionary or brute force. In case of dictionary attack, all possible word combinations will be generated that may be used to decrypt the data which are stored in data storage device or flowing over the network. Challenge-response system is very useful to deal with these sought of problems as explained in [48]. In this protocol, it needs to compute the response when the client tries to access a network and reply back to the server.

Obstacle and Opportunity for Cloud Computing

In recent period, cloud are like a hot cake for the users. But some the organizations are still not confident enough to work with cloud. Some security gap in architecture has made cloud computing untrustworthy with respect to security and privacy [49]. A few issues regarding the limitation of cloud are discussed below:

Privacy and Security

The key of success of an emerging new computing technology depends upon its security standard [50, 51]. In paper [52], authors discussed about some protocol standards for collection, maintenance and disclosure of personality identifiable information. Specific steps should be taken in order to ensure privacy and security in the cloud as discussed in [53, 54].

A public cloud solution turns as a crowd of a number of virtual machines, virtual machine monitors, and supporting middleware [55] etc. It is true that public cloud is much more intruder prone in compare to private cloud due to its shared or openness characteristics. But sometimes private cloud also suffers from some security loopholes. It is important to specify the attack deployment areas which are extensively prone to security attacks and mechanisms ensuring effective client-side and server-side protection for private cloud [56]. Because of the diverse security issues in a public cloud, we prefer private cloud solution compare to public cloud [57]. A secure component model can address the problem of securing mash-up applications. The model also deals with an entropy based security framework for cloud oriented service mash-ups [58, 59].

Performance, Unpredictability, Latency and Reliability

Literature study and experimental report admits that VMs can share CPUs and primary memory in a lucid way in comparison to the network and secondary memory. EC2 instances may vary in their I/O performance rather than primary memory performance [60]. I/O performance can be improved by following ways:

- Improve computer architecture with virtualization technology enabled
- To upgrade operating system with virtualization capability.
- Frequent use of Flash memory as large number of VMs with more I/O operation can sustain in a computer.

Latency [61, 62] is very important parameter in order to store data in cloud. There exist two types of data:

- Time sensitive data
- Non time sensitive data

Time sensitive data refers to mission critical or real time data where immediate response is important by the cloud service providers to the cloud users. Now if the latency is high the n cloud user may face big problem with time sensitive data and here we can think of fog node as a solution. So to handle real time data or time sensitive data cloud providers must be concerned about latency in data processing, maintenance and round trip time management. Latency also plays an important role in case security as well as. Latency should be controlled in every aspect in security in the following manner:

- Time should be reduced to generate security key
- Encryption process should take time as minimum as possible
- Decryption time should be optimized.

On the other hand non sensitive data has the fault tolerance capability so latency is not a big deal here. The overall reliability of cloud depends on the performance, security and quick response.

Portability and Interpretability

Portability of cloud refers to the migration from one cloud service provider to another service provider. If a cloud user is no longer interested to use the service of cloud provider then he or she may go for new service provider for better services or for getting new type services. But this migration process is not very easy as it suffers from following problems [63].

- Heterogeneity is in data format. That means sometimes the data format of a particular cloud provider is not supported by another cloud providers in that case problem may arise.
- Data Structure may be different for two different cloud providers. Languages may not be supported by one cloud providers with other cloud providers.
- Each and every cloud providers have a certain API level which may be different from other cloud providers.

For the above problems some lacuna may be there between two different cloud providers and that causes problem for migration. The problem arise in case of migration process for different type of cloud services is known as lock-in. Lock-in can be different types depending on the cloud service types and some of them are:

- SaaS Lock-in
- PaaS Lock-in
- IaaS Lock-in

Heterogeneity in data format is associated with SaaS Lock-in. It is observed that when cloud user moves their entire data from one cloud providers to another cloud provider, the data to be moved does not fit with the data format provided by new cloud provider. Language mismatching and the API level inequality is related with PaaS lock-in. To avoid this problem every cloud service provider must be open in terms of language and API.

If more and more data pushed to the cloud then data lock-in increases and due to this data overhead on cloud storage lock-in may arise. Lock-in generates in infrastructure level like cloud storage is known as PaaS lock-in. In order to avoid this lock-ins, the customer should be clear about their requirements so that data overhead is less [64]. Data has to be kept in an encrypted form and proper key management techniques must be implemented in order to avoid risk for every cloud models [65]. On the other hand, the cloud users are totally unaware about the location of their data stored in cloud and this is to some extend helps to enhance the security. But simultaneously cloud service providers must be serious about the data so that they become trustworthy in front of the users [66]. A domain specific trust based model has been proposed in [67] to handle security and interoperability in cross clouds.

Data Breach through Optical Fiber

Data communication in cloud takes place via different data centers. In every data center there must be security measures in order to monitor incoming and outgoing data. To transfer data optical fiber can be chosen as best transmission media. Optical fibers are fast and secure enough to deal with issues of cloud computing. But some exception is still there as Telco Verizon's optical network issue was discovered by US Security forces [68].

Data Storage over IP Network

Cloud popularity of networked storage devices are gradually increasing as people prefer internet to store the data to avoid the hassle in hard drives or in storage server. Moreover there are some security risks but still Storage Area Network (SAN) and Network-Attached Storage (NAS) becomes popular due to its storage as a service. Storage network vulnerabilities have been discussed in [68].

Network Accessibility

Cloud provides various type of services to the user and due to its variety, the cloud is become a hot cake for the users. But to get access to the cloud, users must have the internet service available in his or her side. Without internet the popularity of cloud is degradable.

Data Latency

Variation in latency experiences jitter. Now this variation in latency is more in case of unguided media like wireless communication and less in case of guided media like wired communication. In case of wireless network delay or latency varies that means this type of experiences jitter. On the other hand the wired network deals comparatively less variation in latency as it offers dedicated point to point connection.

Dynamic Network Monitoring

Mobile application in mobile cloud must be intelligence enough to adopt with the resources available in a mobile phone. Cloud Application must be capable enough to measure storage capacity, network bandwidth etc.

Confidentiality of Mobile Cloud based Data Sharing

Data confidentiality is very important in case of mobile phone to run cloud application. Sometime malicious cloud application may hack the data from mobile device. Mobile device must be protected with high security password, pattern or face detection techniques.

Better access Control

To get better access control over the data moving around the cloud, followings improvements should be done.

- User authentication and control mechanism must be unique and powerful.
- Explicit partition measurements are needed to overcome the security gaps in virtualization.
- Strong virus-scanning and malware protection software need to be installed in pc and mobile device
- Device identity protection must be there in mobile device.

Data Storage Security

User data is stored in cloud storage. Offering storage area to the cloud user is known as storage as a service. But data may be stolen or data be corrupted by the attacker while it is in cloud storage. So there remains security breach in cloud storage area. The various aspects of data security are as follows:

- Data-at-rest
- Data-in-transit
- Data Lineage
- Data Provenance
- Data Remanence

Data at Rest

Data at rest means that the data is not dynamically moving from one machine to another machine or routing around the network, but data has been kept a flash drive, hard drive, or archived in some other way. The goal of data protection at rest is to protect inactive data stored which are stored on any device or network. While data at rest is sometimes measured to be less vulnerable than data in transit, attackers often try to find the data which is in inactive and it is more valuable target than data in motion. The risk profile of data at rest or data in transit will be depends on measurement of the security that are in place to secure data in either state.

In a shared environment there is a chance to access the data which is in rest in IaaS platform by unauthorized users. But storage devices in IaaS environment with built in encryption techniques can be useful to protect the data at rest. A lockbox approach is also useful to address the above issue. A public encryption scheme has been discussed in [69] to secure data at rest in a cloud computing environment.

Data in Transit

Data in transit, or data in motion, is defined as the data actively stirring from one place to another place such as over the internet or through a private or public network. Data protection is required when data is traveling from one network to another network or being transferred from a local storage space to a cloud storage space. In data transit or wherever data is moving, efficient data safety measures are critical as data is often considered less secure while in motion. To handle data in transit the security techniques should be standardized and up to date with latest security threats as discussed in [70, 71].

Data Lineage

Finding the data route is known as data lineage. It is important for auditing [72] purpose in the cloud. Data lineage is a challenging job in a cloud computing environment especially for public cloud. It is very advantageous to know within an enterprise which has put their data on the cloud that where and when the data was specifically located within the cloud whether the data in the cloud is encrypted or not. Data lineage is confined with three questions as follows:

- Where data comes from
- Where it flows to
- Where it is transformed while it travels through the enterprise.

Data Provenance

Data provenance is to preserve the veracity of the data and ensure that computationally. Classification of provenance techniques and several data provenance techniques have been discussed in [73]. In case of data provenance, the verification of the data stored in provider (server) can be done by users or the owner. Data provenance is more challenging and harder than data lineage. Even data lineage can be recognized in a public cloud for some cloud users but verifying data provenance is more difficult. Here not only integrity of the data is proved, but the more specific provenance of the data. The two terms slightly differ to each other.

Data Remanence

Data Remanence refers to the missing of data in case of data transfer or data removal. However in private cloud data remanence encourages minimal security threats but it causes severe effect in public cloud [74, 75].The ultimate feature of data security is data remanence. Data remanence is the persistent demonstration of data that has been in some way supposedly deleted or removed. This remainder may be due to data being left unbroken by a minimal removing process, or complete physical properties of the storage medium.

ESURING SECURITY AGAINS VARIOUR TYPES OF ATYTACKS

Many end users keep their data in cloud data storage and cloud providers provide the security on those data. Now if the security techniques are not standard then the third party intruder or attacker can easily get the data of end users. In that case, those particular cloud providers are not trustworthy and people will go for other cloud service providers which can provide better security services [24]. Various cloud service delivery specific security threats has been discussed earlier in various paper. Proper identification and then classification of security threat is important prior to implement the security techniques and that can be achieved by rigorous survey on threat. In this section, we have discussed some security technique which ensures the security against the various types of attacks. Most of the state of the art attacks such as Flooding Attack, Side Channel Attack, port scanning, denial of service (DoS), Distributed Denial of Service (DDoS) etc disrupt the services of cloud. We have surveyed various papers to study different types of threat and the corresponding techniques to detect them or prevent them. The well-known attacks and risks of cloud computing are mentioned in the following Table 1 [76]. Table-1 present different thereat which are facing to use the cloud computing services.

Table 1: Threats Categorization

Category	Description	Attacks
Standards of security techniques	It deals with security standards of various security measures in order to protect from threats	Not applicable
Network Level	Denial of service attacks, Distributed denial of service attacks are under network level attacks	Port Scanning, Phishing, Man-In-The-Middle Attack, Denial of service attack
Access Control	Attacks related to authentication, authorization and identification	Cloud Malware Injection attack, Man-In-The-Middle Attack, Phishing
Cloud Infrastructure	SaaS, PaaS and IaaS level including hypervisor attacks	Flooding attack, Denial of service, hypervisor attack, Cloud Malware Injection attack, phishing, Cross VM side channels
Data Level	Data migration, reliability, integrity, confidentiality	Not Applicable

On the basis of literature survey we have enlisted some of the security threats of cloud computing platform and their corresponding probable solutions are also listed below in the following Table-2.

Table 2: Various threats and corresponding solutions

Threat	Description	Methods
Google hacking	Identifies login passwords, pages containing logon portals etc. from the databases	Web Vulnerability Scanner [14].
SQL Injection	In this process some malicious code is injected into a Structure Query Language	Avoid dynamic SQL code, use meta structure, proper user validation, and avoid unwanted data. [29].
Cross Site Scripting (XSS)	injecting mischievous scripts into web based contents	Data Leakage Prevention Technology based on Content, Active Content Filtering, Vulnerability Detection Technology based on Web Application [32]
DoS or DDoS	Denying access to the internet, slowing down the website, unable to give service to legitimate users.	Game theory against bandwidth consuming of DoS and DDoS [75]
IP spoofing	Manipulation of IP packet in order to get unauthorized access user machine or cloud service provider.	Performing filtering for incoming and outgoing packets and enabling encryption for sessions, spoofing attacks can be reduced IPSec based solution.
Sniffer Attack	Unencrypted packets transferring between sender and receiver get captured.	ARP and RTT based solution [36]

Comparative analysis of various security solution of cloud computing platform in terms their advantages and limitations are listed below in Table-3.

Table 3. Comparative study of various security methods in cloud

Methods	Advantages	Shortcomings
Algorithmic protocol for trust ticket deployment [34]	Three levels of verification has been done	It is quite hard to implement when data is in cloud. If the users shares common key then total security system will be collapsed
Dynamic Identity mapping Association and Discovery System [10]	Verified cloud users can access the information	Only validation is not sufficient to implement security mechanism.
FPGA device [45]	The method provides data security with verified attestation under trusted cloud platform	Quite difficult to implement. Complex high quite high.
Dynamic Provable Data possession [51]	Error free audit can be placed.	Not efficient under large data storage
Surveyed on different encryption algorithms [52]	Encryption algorithm can provide security.	Need to be tested on various cloud platform.
Digital signature with RSA algorithm [53]	Very easy to implement under small data storage.	Not efficient under large data storage
Dynamic access control Infrastructure [54]	Security has been provided in virtualized cloud platform	Application level protocol must be checked.
Trusted computing platform with trusted platform model [55]	Trust model can be developed.	Integration of various hardware modules in cloud is quite difficult.
Homomorphic token with distributed verification of erasure-coded data [3]	Storage correctness, Data error localization and identification of misbehaving server.	Issues of fine grained data error localization remain to be addressed.
Border Gateway Protocol [41]	Detects anomaly to ensure that data does not get routed to the wrong system.	This suggested approach does not verify the traffic path but take care the of the routing control messages.

CONCLUSION AND FUTURE SCOPE

In this paper, various security issues of cloud computing and the solutions to overcome the risks have been discussed. Cloud computing which is considered as dominator of the IT market currently has some security risks. Not only security but also there is some issues that need to be controlled along with security threats in cloud computing platform

- How cloud computing framework will be built in order to deal with both structured and unstructured data.
- How migration problem can be dealt with.

Moreover confidentiality and integrity of data should be considered while opting for cloud services from a cloud service provider. Auditing at regular intervals is also mandatory to deal security threats. Errors from cloud service provider side should be minimized. On the basis of the survey carried out in this article, we conclude, that the cloud computing environment cannot provide total security. Groups that are applying cloud computing by increasing their on-premise structure, must be aware of the security challenges faced by cloud computing. To create defense against the cooperation of the agreement integrity and security of their applications and data, defense in depth approach must be applied.

REFERENCES

[1] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", sp. 800-145, pp. 1-3, Sept. 2011. https://pdfs.semanticscholar.org /3ed6/a15029db 533 1928db5a64106d7 cab3ab1dda.pdf

[2] Amazon.com, "Amazon Web Services (AWS)", Online at hppt://aws.amazon.com, 2008.

[3] Con Wang, Qian Wang, KuiRen, and Wenjng Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International Workshop on Quality of service, USA, pp.1-9, 2009, IBSN: 978-42443875-4.

[4] B.P Rimal, Choi Eunmi and I.Lumb, "A Taxonomy and Survey of Cloud Computing Sytem", Intl. Joint Conference on INC, IMS and IDC, 2009, pp. 44-51, Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218.

[5] L. Wang, J. Tao, Kunze M., Castellanos A.C., Kramer D.

and Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, Dalian, China, pp. 825-830, ISBN: 978-0-7695-3352-0, Sep. 2008.

[6] S. Murugesan, "Understanding Web 2.0", IEEE Computer Society, pp. 34-41. July-Aug, 2007. http://91-592722.wiki.uml.edu/file/ view/understanding_web_20.pdf

[7] A. Bakshi and Y. B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, IEEE Computer Society, USA, pp. 260-264, ISBN: 978-0-7695-39614, 2010.

[8] Youseff L., Butrico and M., Silva, D., "Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, Austin, Texas, pp. 1-10, Nov, 2008.

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

[10] B. Wang, Huang He, Yuan, Liu Xiao, Xi Xu and Jing, Min, "Open Identity Management Framework for SaaS Ecosystem," in *ICEBE '09.* pp. 512-517.

[11] S. Subashini and V. Kavitah, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Applications, vol. 34, issue. 1, pp. 1-11, 2011.

[12] F. Elizabeth and Vadim Okun, "Web Application Scanners: Definitions and Functions," in *HICSS 2007,* pp. 280b-280b.

[13] NIST. October, (2010). National Vulnerability Database (NVD). Available: http://nvd.nist.gov/home.cfm

[14] A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", Proceedings of Advances in Computing and Communications, Vol. 193, pp. 445-454, 2011. DOI: 10.1007/978-3-642-22726-4_46

[15] P. Sharma, S. K. Sood and S. Kaur, "Security Issues in Cloud Computing", Proceedings of High Performance Architecture and Grid Computing, Vol. 169, pp. 36-45, 2011. DOI: 10.1007/978-3-642-22577-2_5

[16] Wayne Jansen and Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144, 2011. http://csrc.nist.gov/ publications/drafts/800-144/Draft-SP-800-144_cloud-comput ing.pdf.

[17] Sudharsan Sundararajan, Hari Narayanan, Vipin Pavithran, Kaladhar Vorungati and Krishnashree Achuthan, "Preventing Insider attacks in the Cloud", Communications in Computer and Information Science, vol. 190, issue. 5, pp. 488-500, 2011. DOI: 10.1007/978-3-642-22709-7_48

[18] Thomas W. Shinder, "Security Issues in Cloud Deployment models", TechNet Articles, Wiki, Microsoft, Aug, 2011. http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud-deployment-models.aspx

[19] E. Mathisen, "Security Challenges and Solutions in Cloud Computing", Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 208-212, June, 2011, ISBN: 978-1-4577-0871-8, DOI:10.1109/DEST.2011.5936627.

[20] Alessandro Perilli and Claudio Criscione, "Securing the Private Cloud", Article on Secure Networks, Virtualization.info. http://virtualization.info/en/security/privatecloud.pdf

[21] A. Marinos and G. Briscoe, ―Community cloud computing,‖ In: Cloud Computing (pp. 472-484). Springer Berlin Heidelberg, 2009.

[22] X. G. Condori, Y Sociedad and Revista de "Community cloud computing, Información Teconología, 70-72, 2013.

[23] Sato H., Kanai A. and Tanimoto S, "A Cloud Trust Model in a Security Aware Cloud", Intl. Symposium on Applications and the Internet (SAINT), pp. 121-124, July, 2010, Seoul.

[24] Ryan K. L. Ko, Bu Sung Lee and Siani Pearson,"Towards Achieving Accountability, Auditability and Trust in Cloud Computing", Communications in Computer and Information Science, Vol. 193(4), pp. 432-444, 2011. DOI: 10.1007/978-3-642-22726-4_45.

[25] "Amazon Web Services: Overview of Security Processes", Whitepaper, May, 2011. http://d36cz9buwru1tt. cloudfront.net/pdf/AWS_Security Whitepaper.pdf

[26] Ruixuan Li, Li Nie, Xiaopu Ma, Meng Dong and Wei Wang, "SMEF: An Entropy Based Security Framework for Cloud-Oriented Service Mashup", Int. Conf on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 304-311, Nov, 2011.DOI: 10.1109/TrustCom.2011.41

[27] Pradnyesh Rane, "Securing SaaS Applications: A Cloud Security Perspective for Application Providers", Information Security Management Handbook, Vol. 5, 2010.http:// www.infosectoday. com/Articles/Securing_SaaS Applications.htm

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

[29] A. Liu, Y. Yuan and A. Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009, Honolulu, Hawaii, U.S.A.

[30] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis", Proceedings of the Network and Distributed System Security Symposium (NDSS'07), February, 2007.

[31] Adam A Noureddine and Meledath Damodaran, "Security in Web 2.0 Application Development", iiWAS '08, Proc. of the 10th International Conference on Information Integration and Web-based Applications & Services, pp. 681-685, 2008, ISBN: 978-1-60558- 349-5, DOI: 10.1145/1497308.1497443.

[32] Ter Louw and M. Venkatakrishnan, "BluePrint: Robust Prevention of Cross-Site scripting attacks for existing browsers", 30th IEEE Symposium on Security and Privacy, pp. 331-346, May, 2009. DOI: 10.1109/SP.2009.33

[33] Jonathan Katz, "Efficient Cryptographic Protocols Preventing Man in the Middle Attacks", Doctoral Dissertation submitted at Columbia University, 2002, ISBN:0493509275.http: //www.cs.ucla.edu/~rafail/STUDENTS/katzthesis.pdf

[34] Gurdev Singh, Amit Sharma, Manpreet Singh Lehal, "Security Apprehensions in Different Regions of Cloud Captious Grounds", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[35] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve, "Cloud computing security: Routing and DNS security threats". http://sear chsecurity .techtarget. com/tip/0,289483,sid14_gci1359155_mem1, 00 .html/

[36] Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech and Mounir Frikha, "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004, ISBN: 0-7695-2068-5.

[37] T. Mather, S. Kumarawamy and Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance", O'Reilly Media, ISBN: 978-059-6802769, September 2009, http://oreilly.com/catalog/9780596802776.

[38] K. Vieira, A. Schulter, C. B. Westphall and C. M.Westphall, "Intrusion detection techniques for Gridand Cloud Computing Environment", IT Professional,IEEE Computer Society, vol. 12, issue 4, pp. 38-43,2010. DOI: 10.1109/MITP.2009.89.

[39] Chi-Chun Lo, Chun-Chieh Huang and Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.

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

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

[42] Scalable Security Solutions, Check Point Open Performance Architecture, Quad-Core Intel Xeon Processors, "Delivering Application-Level Security at Data Centre Performance Levels", Intel Corporation, Whitepaper, 2008. http:// download.intel. com/netcomms/technologies/ secu rity/ 320 92 3.pdf

[43] Shengmei Luo, Zhaoji Lin, Xiaohua Chen, ZhuolinYang and Jianyong Chen, "Virtualization security for cloud computing services", Int. Conf on Cloud and Service Computing, pp. 174-179, Dec, 2011.DOI: 10.1109/CSC.2011.6138516

[44] Jenni Susan Reuben, "A Survey on Virtual MachineSecurity", Seminar of Network Security, Helsinki University of Technology, 2007. http://www.tml.tkk.fi/Publications/C/25/ papers/ Reuben_ final. pdf?q=attacks-on-virtual-machine-emulators

[45] Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech and Mounir Frikha, "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004, ISBN: 0-7695-2068-5.

[46] Kellep Charles, "Google's Gmail Hacked by China Again", SecurityOrb, The Information Security knowledge-Base Website, June 2, 2011. http://securityorb. com /2011/06/ googles-gmail-hackedby-china-again/

[47] Antero Taivalsaari, "Mashware: The Future of Web Applications", Technical Report, Feb 2009.http://labs. oracle.com/techrep/2009/smli_tr-2009-181.pdf DOI: 10.1145/1878537.1878703

[48] V. Kumar, M. Singh, A. Abraham and S. Sanyal,"CompChall: addressing password guessing attacks", Int. Conference on Information Technology: Coding and Computing, pp. 739-744, vol. 1, April, 2005.

[49] Md Tanzim Khorshed, A. B. M. Shawkat Ali and Saleh A. Wasimi, "Trust Issues that create threats for Cyber attacks in Cloud Computing", IEEE 17th International Conference on Parallel and Distributed Systems, pp. 900-905, 2011.

[50] S. Pearson, "Taking account of privacy when designing cloud computing services", CLOUD '09 Proc. of ICSE Workshop on Software Engineering Challenges of Cloud Computing, pp. 44-52, IEEE Computer Society Washington, DC, USA, May 2009. ISBN: 978-1-4244-3713-9.

[51] George V. Hulme, "NIST formalizes cloud computing

definition, issues security and privacy guidance", Feb. 3, 2011 [A common platform enabling security executives to share best security practices and strategic insights]. http://www. csoonline.com/article/661620/nistformalizes- cloud-com puting -definition-issuessecurity- and-privacy guidance.

[52] Julisch K., and Hall M., "Security and control in the cloud", Information Security Journal: A Global Perspective, vol. 19, no. 6, pp. 299-309, 2010.

[53] Chi-Chun Lo, Chun-Chieh Huang and Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.

[54] Hamid R. Motahari-Nezhad, Claudio Bartolini, Sven Graupner, Sharad Singhal and Susan Spence, "IT Support Conversation Manager: A Conversation-Centered Approach and Tool for Managing Best Practice IT Processes", Proceedings of the 2010 14th IEEE International Enterprise Distributed Object Computing Conference, pp. 247-256, October 25-29, 2010, ISBN: 978-1-4244-7966-5.

[55] L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture", ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009. DOI: 10.1109/ICWS.2009.144.

[56] Wayne Jansen, Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/ drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.

[57] Jon Marler, "Securing the Cloud: Addressing Cloud Computing Security Concerns with Private Cloud", Rackspace Knowledge Centre, March 27, 2011, Article Id: 1638. http://www.rackspace.com/knowledge_center/privatecl oud/ securing-the-cloud-addressing-cloud-computingsecurity- concerns-with-private-cloud

[58] Frederik De Keukelaere, Sumeer Bhola, Michael Steiner, Suresh Chari and Sachiko Yoshihama, "Smash: secure component model for cross-domain mashups on unmodified browsers", Proc. of the 17th International Conference on World Wide Web, ACM, NY, USA, 2008, ISBN: 978-1-60558-085-2, DOI: 10.1145/1367497.1367570.

[59] Ruixuan Li, Li Nie, Xiaopu Ma, Meng Dong and Wei Wang, "SMEF: An Entropy Based Security Framework for Cloud-Oriented Service Mashup", Int. Conf on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 304-311, Nov, 2011.DOI: 10.1109/TrustCom.2011.41

[60] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Petterson, Ariel Rabkin, Ion Stoica and Matei Zaharica, "A View of Cloud Computing", Communications of the ACM, vol. 53, issue. 4, April 2010, USA. DOI: 10.1145/1721654.1721672

[61] Neal Leavitt, "Is Cloud Computing Really Ready for Prime Time?" Computer, vol. 42, issue. 1, pp. 15-20, IEEE Computer Society, CA, USA, January 2009. ISSN: 0018-9162.

[62] Robert Minnear, "Latency: The Achilles Heel of Cloud Computing", March 9, 2011, Cloud Expo: Article, Cloud Computing Journal. http://cloudcom puting.sys con.com /node/1745523.

[63] Daniele Catteddu and Giles Hogben, "Cloud Computing: Benefits, Risks and Recommendations for Information Security", European Network and Information Security Agency (ENISA), Nov, 2009. http://www.enisa.europa.eu/act/ application security/ test/act/rm/files/deliverables/ cloudcomputing - risk assessment

[64] Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis and 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. DOI: 10.1109/MIC.2009.103.

[65] Michael Kretzschmar and S Hanigk, "Security management interoperability challenges for collaborative clouds", Systems and Virtualization Management (SVM), 2010, Proceedings of the 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and the Cloud, pp. 43-49, October 25-29, 2010. ISBN: 978-1-4244-9181-0, DOI: 10.1109/SVM.2010.5674744.

[66] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues", 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[67] W. Li, L. Ping and X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment", 2010 International Conference on Electronics and Information Engineering (ICEIE), Volume: 1, pp. V1-14 - V1-19, 2010. DOI: 10.1109/ICEIE.2010.5559829.

[68] Jessica T., "Connecting Data Centres over Public Networks", IPEXPO.ONLINE, April 20, 2011. http://online.ipexpo. co.uk/2011/04/20/connectingdata-centres-over-public-net works/

[69] Jeff Sedayao, Steven Su, Xiaohao Ma, Minghao Jiang and Kai Miao, "A Simple Technique for Securing Data at Rest", Lecture Notes in Computer Science, pp. 553-558, 2009. DOI: 10.1007/978-3-642-10665-1_51

[70] R. A. Vasudevan, A. Abraham, S.Sanyal and D.P. Agarwal, "Jigsaw-based secure data transfer over

computer networks", Int. Conference on Information Technology: Coding and Computing, pp. 2-6, vol.1, April, 2004.

[71] R. A. Vasudevan and S. Sanyal, "A Novel Multipath Approach to Security in Mobile Ad Hoc Networks (MANETs)", Int. Conference on Computers and Devices for Communication, CODEC'04, Kolkata, India.

[72] Sudharsan Sundararajan, Hari Narayanan, Vipin Pavithran, Kaladhar Vorungati and Krishnashree Achuthan, "Preventing Insider attacks in the Cloud", Communications in Computer and Information Science, vol. 190, issue. 5, pp. 488-500, 2011. DOI: 10.1007/978-3-642-22709-7_48

[73] Yogesh L. Simmhan, Beth Plale and Dennis Gannon, "A Survey of Data Provenance Techniques", ACM SIGMOD, vol. 34, issue. 3, Sep, 2005, NY, USA. DOI: 10.1145/1084805.1084812

[74] P. R. Gallagher, "Guide to Understanding Data Remanence in Automated Information Systems", The Rainbow Books, ch3 and ch.4, 1991.

[75] 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. http://www.techrepublic.com /blog/security/epsilondata- breach-whats-the-value-of-an-em ail-address/5307

[76] I. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey," Computers, vol. 3, no. 1, pp. 1–35, Feb. 2014.

[77] Qishi Wu, Sajjan Shiva, Sankardas Roy, Charles Ellis and Vivek Datla, "On Modelling and Simulation of gametheory based defense mechanisms against DoS and DDoS attacks", Proceedings of 2010 Spring Simulation Multiconference, NY, USA, 0032010. DOI: 10.1145/1878537.1878703.